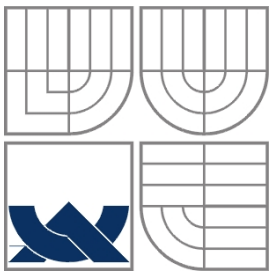
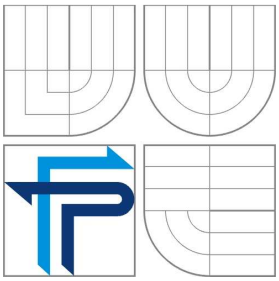


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
DEPARTMENT OF INFORMATICS

MODEL PRÁCE S DOKUMENTY V ELEKTRONICKÉM OBCHODOVÁNÍ

MODEL EDI IN E-COMMERCE

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — JIŘÍ GROHMANN
AUTHOR

VEDOUCÍ PRÁCE — PROF. ING. JIŘÍ DVOŘÁK, DRSC.
SUPERVISOR

BRNO 2007

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2007/08
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Grohmann Jiří

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Model práce s dokumenty v elektronickém obchodování

v anglickém jazyce:

Model EDI in e-commerce

Pokyny pro vypracování:

Úvod
Vymezení problému, cíle práce a informační zdroje
Teoretická východiska práce
Analýza problému a současný stav řešené problematiky
Vlastní návrhy řešení, přínos návrhů řešení, ekonomické hodnocení
Závěr
Použité informační zdroje
Přílohy

Podle § 60 zákona č.121/2000 Sb. (autorský zákon) v platném znění, je tato práce „Školním dílem“. Využití této práce se řídí právním režimem autorského zákona. Citace povoluje Fakulta podnikatelská Vysokého učení technického v Brně. Podmínkou externího využití této práce je uzavření “Licenční smlouvy“ dle autorského zákona.

A b s t r a k t

Tato práce obsahuje model práce s dokumenty elektronického obchodování. Je zde rozebrána možnost elektronických podpisů v účetnictví a popsány vybrané případy bezpečnosti elektronického podpisu. V práci jsou uvedeny vybrané možnosti ochrany dat v elektronickém obchodování.

A b s t r a c t

This work is containing a model EDI in e-commerce. There is a situation about electronic signatures in the accounting is taking to parts and chosen cases of safety of electronic signature. In this work are chosen possibilities of protecting data in the e-commerce.

Klíčová slova	**[Primary word]**
Elektronický podpis	[General electronic signature]
Elektronické obchodování	[E-commerce]
Ochrana dat	[Data security]
Autentizace	[Authenticity]
Integrita dokumentu	[Integrity documents]
Certifikační autorita	[Certificate authority]
Bezpečnost e-podpisu	[E-signature safety]
Zaručený elektronický podpis	[Advanced electronic signature]
Kvalifikovaný certifikát	[Qualified certificate]
Komunikační protokoly	[Communication protocol]
Firewall	[Firewall]
Elektronický dokument	[Electronic document]
Rozhraní	[Port]
Bezpečnost	[Safety]
Struktura souboru	[Construction file]

Bibliografické citace:

GROHMANN, J. *Model práce s dokumenty v elektronickém obchodování*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2007. 83 s. Vedoucí bakalářské práce Prof. Ing. Jiří Dvořák, DrSc.

Prohlášení:

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů.

Brno, 20. května 2008

……
podpis

Poděkování:

Chtěl bych poděkovat především svému vedoucímu práce Prof. Ing. Jiřímu Dvořákovi, DrSc. za jeho ochotu a rady na konzultacích a při psaní této práce. A tím výraznou měrou přispěl k úspěšnému dokončení mé práce.

OBSAH

SEZNAM OBRAZKŮ A TABULEK

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

PGP	Pretty Good Privacy
RFC	Request For Comment
PC	Personal Computer
PIN	Personal Identification Number
USB	Universal Seriál Bus
MD	Message Digest
SHA	Secure Hash Algorithm
NIST	National Institute for Standards and Technology
RSA	Rivest –Shamir –Adleman
DSA	Digital Signature Algorithm
PK	Private Key
CRL	Certificate Revocation List
ID	IDentification
CA	Certification Authority
ITU	International Telecommunication Union
SSL	Secure Sockets Layer
FTP	File Transfer Protocol
DoS	Denial of Service
DDoS	Distributed DoS
HTTP	Hyper Text Transfer Protocol
RLP	Remote line Printing
HP	Hewlett Packard
TCP	Transmission Control Protocol
IP	Internet Protocol
UDP	User Datagram Protocol
POP	Post Office Protocol
CD	Compact Disc
E-	Electronic
URL	Uniform Resource Locators
XML	eXtensible Markup Language

POST	Power On Self Test
PKC	Public Key Cryptography
ASCII	American Standard Code for Information Interchange
ISO	International Organization for Standardization
HTTPS	Hyper Text Transfer Protocol – Secure
W3C	World Wide Web Consortium
EDI	Electronic data interchange
AIX	Advanced Interactive eXexutive
SW	Software
HW	Hardware
IBM	International Business Machines
PKI	Public key infrastructure
IZS	Integrovaný záchranný systém
SDK	Software Development Kit
SSO	Single Sign On
IEC	International Electrotechnical Commision
API	Application Programming Interface
CSP	Certified Systems Professional
ČDS	Česká daňová správa
ZAREP	Zaručený elektronický podpis
OSN	Organizace Spojených Národů
MFČR	Ministerstvo financí České republiky

1. ÚVOD

Elektronické obchodování chápeme jako běžnou výměnu zboží, služeb či informací pomocí elektronického média. Vzniklo v poměrně nedávné minulosti a můžeme také říci, že i dnes je teprve ve svém počátečním vývojovém stádiu. První pokusy začaly již před mnoha lety, především v oblasti výměny dokumentů či zprostředkováním platebního styku. S rozvojem Internetu se všechny možnosti těchto aktivit zmnohonásobily, přibyly další aktivity a elektronicko-ekonomické podnikání se stalo novým modelem obchodování, schopným samostatné existence.

V současné době se stává tato forma využití Internetu velice využívanou i v České republice. Prvenství v obchodování prostřednictvím Internetu patří USA. Tam probíhá 80% světového elektronického obchodu. Pouze 20% se odehrává ve „zbytku" světa.

Jedním z hlavních důvodů prvenství USA jsou dobré zkušenosti potencionálních i skutečných klientů této služby s fungováním vztahu objednavatel – dodavatel, propracovaný a jednoduchý způsob placení, možnost vracení zboží atd. Důvodem, proč Evropa, zaostává je zřejmě z určitého evropského konzervatismu, projevující se potřebou osahat si kupované zboží. A to v České republice při její kupní síle platí dvojnásob.

V dnešní době zahrnuje využití Internetu ve sféře podnikání několik oblastí:

- *Příprava trhu na cílenou reklamu informacemi a semináři. A to nejen přípravou manažerů, ale také přípravou a zpravováním co největší skupiny obyvatel, potencionálních zákazníků.*
- *Systémy elektronicky řízeného podnikání i řízení lidí zabývajících se službami, prodejem a oběhem zboží.*
- *Organizaci projektů sloužících k rozvoji elektronického podnikání, vytváření podmínek pro uplatnění středních a malých firem.*

Ačkoli se dnes elektronické platby vyznačují velmi vysokou kvalitou zabezpečení, jsou zde i hrozby zneužití a falzifikace[1]. Proto tato práce bude zaměřena na elektronický podpis a bezpečnost dat v elektronickém obchodování. Analýza tohoto specifického druhu podpisu bude práce sledovat v odvětví ekonomicky-účetnickém.

[1] Falzifikace – napodobení, padělání něčeho

2. VYMEZENÍ PROBLÉMU, CÍLE PRÁCE A INFORMAČNÍ ZDROJE

2.1 VYMEZENÍ PROBLÉMU

Rozvoj informačních technologií je přirozeným znakem vývoje naší společnosti. V posledních letech se věnuje velká pozornost elektronickému obchodování (dále e-obchodování). Lze považovat, že tento jev ovlivnil obrovskou mírou Internet, který stal fenoménem dnešní doby. Počítač se stal běžnou součástí našeho každodenního života, stejně jako používání Internetu. ČDS[2] tak poskytla možnost podávat daňová přiznání elektronicky.

ČDS založila daňový portál na internetových stránkách, který umožňuje uživatelům získat informace osobních daňových účtů. Daňový portál pracuje s reálnými údaji, které jsou vedeny u jednotlivých finančních úřadů. Je nutné dbát na dodržení bezpečnosti přístupu k těmto údajům. Podmínkou pro komunikaci se statní správou pomocí elektronického podpisu je tzv. kvalifikovaný certifikát. Tento zaručený elektronický podpis (dále ZAREP) se přikládá k aplikaci EPO (elektronického podání), která umožňuje zpracovávat daňová přiznání elektronicky. E-dokument prochází nezabezpečenou sítí Internetem. Zde se nacházejí prostředky, jež mohou ohrozit bezpečnost únikem dat v e-dokumentu.

2.2 CÍLE PRÁCE

Cílem práce je model práce s dokumenty v elektronickém obchodování. Tento model práce je zaměřen především na elektronický podpis v e-dokumentech, jež v dané problematice slouží k identifikaci identity uživatele-zákazníka během komunikace mezi státní správou a občany. Dalším cílem rozbor elektronických podání (EPO), jež plní funkci daňového přiznání v digitální podobě.

Bezpečnost informací je v poslední době hodně řešenou problematikou. Vývoj informačních technologií spolu s vývojem Internetu vytváří nové hrozby pro zabezpečený systém. Proto dalším cílem je nalezení účinné metody ochrany dat.

[2] Česká daňová správa – orgán státní správy ČR, který řídí správu daní a ve stanoveném rozsahu se podílí na jejím výkonu.

Cílem je vymezit:

- *Princip fungování elektronického podpisu.*
- *Analýza EPO (elektronického podání).*
- *Účinnou metodu ochrany dat.*

2.3 INFORMAČNÍ ZDROJE

Vznik a rozšíření nových elektronických médií znamenalo dokonalejší a rychlejší možnosti pro rozšiřování informací publikované pouze v tištěné podobě. Termín elektronické informační zdroje lze popsat jako publikace nakladatelů v existujících formách, které se přizpůsobují novým trendům a technologiím informační infrastruktury.

Základní prameny použití informací:

I) Publikace v tištěné podobě (literatura, Novinové články, Časopisy)
II) Dokumenty v elektronické podobě, včetně článků a knih
III) Referenční údaje (např. slovníky a encyklopedie)
IV) Semináře, Prezentace
V) Konference
VI) E-learnigové kurzy
VII) Virtuální knihovny

Pozn. : Nalezené informační zdroje se nachází v příloze A.

3. TEORETICKÁ VÝCHODISKA PRÁCE

3.1 ELEKTRONICKÁ KOMUNIKACE

Počátky elektronické komunikace se datují již od 70. Let. Jako první se v praxi uplatnil systém čárkových kódů, od 80. Let se k nim přidalo EDI[3]. Elektronická komunikace se stala nezbytnou pro fungování kterékoliv organizace. Tvoří základ pro celkový růst ekonomiky a vytváří podmínky pro vznik a fungování tzv. informační společnosti. S obrovským rozvojem e-komunikací a technologií v Evropě i ve světě umožňují zavádění nových služeb a vytvářejí se tak předpoklad pro přechod ke globální informační společnosti propojené sítí.

Elektronická komunikace jsou společným označením pro konvergenci sektorů telekomunikací, mediálních a informačních technologií. Konvergence[4] je výrazným průvodním jevem rozvoje těchto sektorů a podmiňuje naplnění cílů stanovených Evropským summitem v r. 2000 v Lisabonu a podle předpokladů by se měla EU v roce 2010 nejvíce konkurenčně schopnou ekonomikou na světě. Elektronická komunikace a dokumentace zdaleka není jen otázkou technickou, ale také organizační.

Možnosti elektronické komunikace mezi dvěma subjekty:

- *Individuál – individuál*
- *Systém A – Systém A*
- *Systém A – převodní tabulka – systém B*
- *Standard – standard*

3.2 ELEKTRONICKÉ DOKUMENTY

Elektronické dokumenty mají mnoho výhod. Jsou známé již více než 10 let a byly shrnuty do termínu „ bezpapírová kancelář“. Dalším impulzem byla digitalizace při zavedení I. Certifikační autority v roce 2002 a tím reálné možnosti podepisovat e-podpisem. Dá se předpokládat, že usnadnění a zrychlení manipulace s ED spolu se silným ekonomickým tlakem, způsobí během několika málo let, že tištěné dokumenty zcela zmizí.

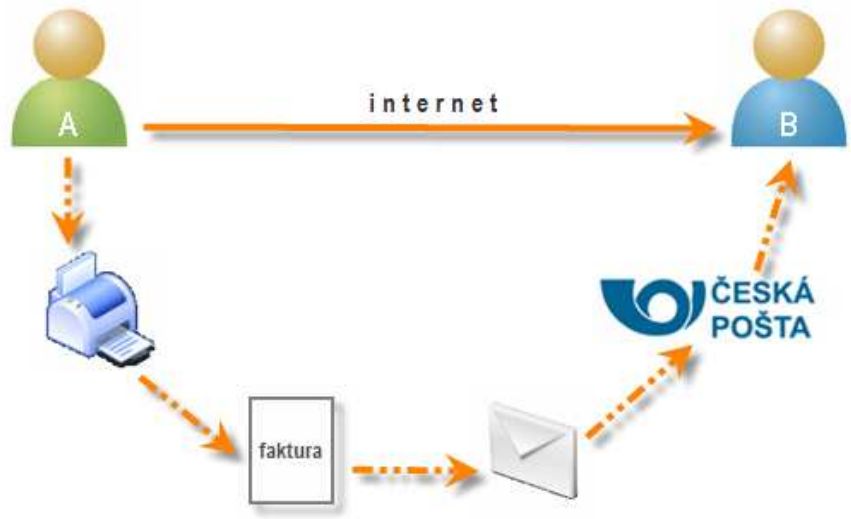
Přesto, že existuje podpora zákona a příslušné technologie jsou dostupné, je stále velké množství dokladů vyhotovováno a zasíláno v papírové podobě. V České republice je

[3] EDI (elektronická výměna dat) – jedná se o výměnu strukturovaných zpráv mezi počítači, respektive mezi počítačovými aplikacemi a je nejpoužívanějším datovým formátem pro elektronické obchodní transakce.

[4] Konvergence – sbíhavost, sblížení (popř. vývoj, který vede ke sblížení)

ročně vydáváno přibližně 700 miliónů faktur, polovina má papírovou podobu. Elektronická forma dokladu má řadu výhod, mezi které patří zejména zpracování, jednoduchá manipulace, výpočetní operace. Účetní doklady jsou dnes převážně zpracovávány na počítači, ale stále existuje poměrně velká část uživatelů, kteří stále preferují odesílání dokladů svým partnerům v papírově podobě, archivaci účetních dokladů v papírové formě, atd.

Obr. A 1: Přenos dokladu mezi dvěma subjekty.[5]



Obr. A 2: Tok dokladů mezi dvěma subjekty.[6]

[5] Papírový versus elektronický dokument. *ISVS* [online]. 2007 [cit. 2008-05-01]. Dostupný z WWW: http://www.isvs.cz/e-podpis-podatelny/papirovy-versus-elektronicky-dokument-27-dil.html.

[6] Papírový versus elektronický dokument. *ISVS* [online]. 2007 [cit. 2008-05-01]. Dostupný z WWW: http://www.isvs.cz/e-podpis-podatelny/papirovy-versus-elektronicky-dokument-27-dil.html.

Elektronický dokument můžeme chápat jako datový soubor, která je spojena s komunikací či přenosem mezi odesílatelem a příjemcem, komunikací mezi podniky, tak i vnitřní oběh dokladů v podniku nebo komunikací s úřady státní správy apod.

Výhody ED:

- *Úspora nákladů na vyhotovení dokladu*
- *Úspora nákladů za poštovné*
- *Úspora lidské práce*
- *Zrychlení komunikace*
- *Automatizace účetnictví*
- *Zpřehlednění procesů*
- *Zamezení vzniku chyb*
- *Zkrácení doby splatnosti faktur*
- *Usnadnění a urychlení kontroly*
- *Šetrnost k životnímu prostředí*
- *Napojení na elektronický platební styk*

Nevýhody ED:

- *Ochrana dokumentů*
- *Zabezpečení dokumentu*
- *Finanční náročnost zavedení*

3.3 HISTORIE ELEKTRONICKÉHO PODPISU

Pojem digitální podpis vznikl souběžně se vznikem asymetrické kryptografie v druhé polovině sedmdesátých let. Elektronický podpis tak jak ho známe dnes je obecnějším pojmem než digitální podpis. E-podpis nabízí kromě samotného digitálního podpisu také biometrické metody, které jsou proto vhodné pro použití v legislativních dokumentech a pro komunikaci s orgány státní správy.

V rámci komise OSN[7] pro mezinárodní obchodní právo (UNCITRAL) byl zpracován Vzorový zákon o elektronickém obchodu, který byl odsouhlasen v roce 1996.

V prosinci roku 1999 schválil Evropský parlament a Rada Evropské unie Směrnici 1999/93/EC pro elektronické podpisy v rámci společenství s cílem usnadnit používání elektronických podpisů a přispět k jejich právnímu uznání v prostředí členských států EU.

V České republice nabyl Zákon 227/2007 Sb. o elektronickém podpisu účinnosti 1. 10. 2000. V tomto zákoně je definován zaručený elektronický podpis a podmínky jeho používání.

V dnešní době se dokončují Obecná pravidla UNCITRAL[8] pro elektronické podpisy, které mají sjednotit především právní aspekty elektronických podpisů, certifikačních orgánů a certifikátů v celosvětovém měřítku.

Tímto krokem byla odstartována nová podoba internetové ekonomiky. Zrovnoprávnily papírové a elektronické dokumenty, což vytvořilo ideální předpoklady pro rozvoj elektronického podnikání v ČR.

3.4 PGP (Preety Good Privacy) – ŠIFROVACÍ STANDARD

PGP ve své první verzi bylo vytvořeno Phillipem R. Zimmermannem v roce 1991. V roce 1996 byla založena společnost *PGP, Inc.*, která je posléze koupena firmou *Network Associates Inc*. PGP se postupem času stalo de facto standardem pro šifrovanou komunikaci.

Vznikem standardu *OpenPGP (RFC 2440)* je dalším krokem k nezávislosti PGP na jednom konkrétním výrobci. Existuje v několika komerčních i volně dostupných verzí, byly vyvinuty speciální plug-iny[9] pro většinu poštovních klientů, které umožňují automatické šifrování či podepisování odesílaných zpráv.

PGP řeší rozpor mezi těmito požadavky: rychlost a kvalitou šifrování. Toto řeší „drobnou fintou“, pro vlastní šifrování se používá symetrický klíč dostatečné délky, který je vygenerován zcela náhodně pro každá přenášená data. Tento klíč je pak zašifrován silnou asymetrickou šifrou a přibalen ke zprávě. Program příjemce tedy

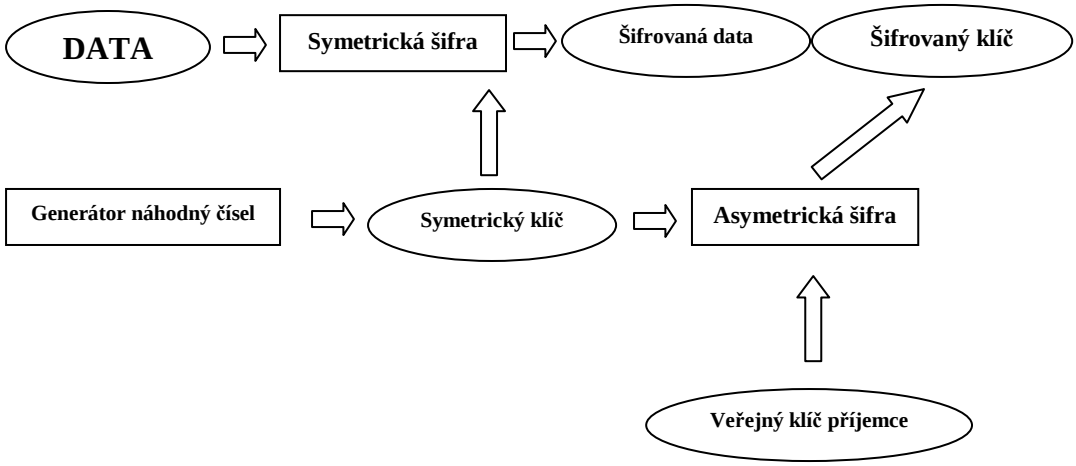
[7] OSN (Organizace spojených národů) – je mezinárodní organizace, jejímž cílem je zachování mezinárodního míru, bezpečnosti a zajištění mezinárodní spolupráce.
[8] UNCITRAL (Komise OSN pro mezinárodní obchodní právo) – cílem je pomáhat odstraňovat překážky mezinárodního obchodu.
[9] Plug-iny – jedná se o zásuvné moduly, které slouží k rozšíření funkčnosti (např. programu, her atd.).

nejprve dešifruje klíč a poté jim dešifruje vlastní zprávu. K nahrazení místa, které přibalením klíče zabereme, je přednášený text komprimován.
PGP používá algoritmy symetrického i asymetrického šifrování, přičemž spojuje výhody obou.

Každý uživatel šifrování musí mít své dva klíče:

- *Klíč, jehož pomocí se zprávy šifrují, se nazývá veřejný klíč, protože jej uživatel musí poskytnout svým partnerům. Ti klíč musí znát a používat ho k zašifrování zpráv právě tomuto uživateli, který bude příjemcem zprávy. Jiní ji nemohou rozšifrovat.*
- *Klíč, kterým se zprávy u příjemce dešifrují, je pouze jediný a nesmí se poskytnout 3 osobě. Nazývá se soukromým klíčem. Je to jediný nástroj, který došlou zprávu může rozšifrovat. To nemůže udělat ani odesílatel. Jakmile zprávu veřejným klíčem zašifruje, už do ní nemůže zasáhnout.*

Obr. A 3: Princip činnosti programu PGP [10]

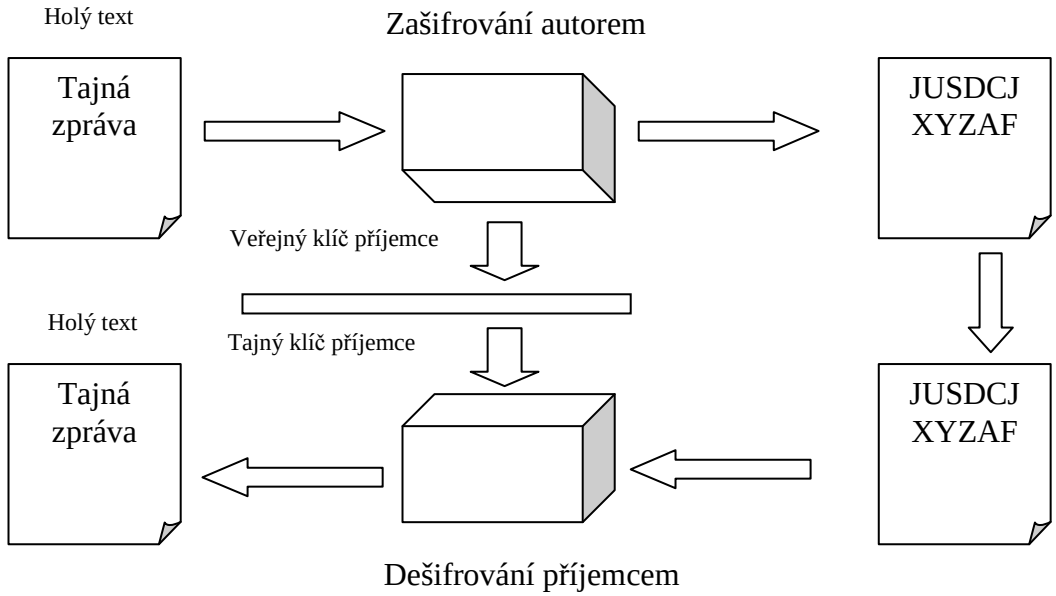


Pravost klíčů může být ohrožena nesprávným způsobem jejich předání. Dalším nebezpečím je uložení klíče v PGP. Tam je chráněn heslem a tomu musí věnovat dostatečnou pozornost. Heslo by mělo být dostatečně odolné před hackery, heslo musí být dostatečně dlouhé a složitě vytvořené.

[10] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. Vydání, Brno: Computer Press, 2004. ISBN 80-251-0106-1.

Chceme-li zasílat zprávy vybraným příjemcům (adresátům), musí také oni mít svůj pár klíčů. Veřejný nám musí poskytnout, soukromým si došlou zprávu dešifrují. Proto potřebujeme *Kroužek klíčů* – tak je nazýván soubor, kde se shromažďují veřejné klíče.

Obr. A 4: Schéma asymetrického šifrování [11]



Na schématu můžeme sledovat cestu tajné zprávy z vlastního PC příjemci. Zpráva je zašifrovaná Veřejným klíčem příjemce. Takto upravená zpráva cestuje „nebezpečným územím“ k příjemci. Ten svým Tajným klíčem příjemce zprávu rozšifruje a získá původní text.

Šifrování spolu s elektronickým podpisem pozitivně ovlivňují celou oblast bankovnictví, elektronický obchod i elektronickou poštu.

3.5 ELEKTRONICKÝ (DIGITÁLNÍ) PODPIS

Pojmy elektronický podpis a digitální podpis budeme považovat za synonyma[12], i když podle některých právních úprav se jedná o zcela odlišné věci. Elektronický podpis můžeme popsat jako elektronické údaje autora nebo jinak řečeno odesílatele dokumentu, připojené k němu. V širším významu se za elektronický podpis považuje uvedení nešifrovaných identifikačních údajů (můžeme zmínit, že se jedná o např. jména, adresy nebo jakékoli identifikační číslo atd.) na konci textu v digitální podobě,

[11] KRAS, P. *Internet v kostce*. 2. Vydání, Havlíčkův Brod: Fragment, 2002. ISBN 80-7200-510-3.

[12] Synonyma – označuje slovo, které zní jinak, ale má stejný nebo podobný význam.

které zaručuje jednoznačné určení označené osoby. Nejedná se ovšem o integritu podepsaného dokumentu, ani autentizaci podepsaného. Elektronický podpis označuje fyzickou osobu, která jedná svým jménem, jménem právnické osoby nebo jejího orgánu. Elektronická značka může označovat i právnickou osobu nebo organizační složku státu.

3.5.1 ZARUČENÝ ELEKTRONICKÝ PODPIS

Zaručený elektronický podpis můžeme považovat v takové formě, která pomocí kryptografických metod zaručuje integritu dokumentu a autentizaci podepsaného. Navíc pro některé účely je vyžadován zaručený elektronický podpis pouze s předepsanými typy certifikace (neboli „založený na kvalifikovaném certifikátu“). V současné době se však zaručený elektronický podpis využívá stále více i ve státní sféře, i přes nevoli některých úřadů přizpůsobit se novým technologiím.

Obr. A 5: Řetězec znaků představující elektronický podpis[13]

```
-----BEGIN PGP SIGNATURE-----
Version PGPfreeware 6.5.3 for non-commercial use <http://www.pgp.com>
IQA/AwUBOcshhx8J2G6UPaBwEQKeYwCeNpw/5io098plCsJRwENcYdrWzNIAo
LQR
tJJd0GJ1VzXrxkG68kuZggg1
=Infu
-----END PGP SIGNATURE-----
```

Rozdíl mezi prostým a zaručeným elektronickým podpisem je podobný rozdílu mezi úředně neověřeným a ověřeným vlastnoručním podpisem.

[13] KRAS, P. *Internet v kostce*. 2. Vydání, Havlíčkův Brod: Fragment, 2002. ISBN 80-7200-510-3.

Zaručený elektronický podpis zajišťuje:

- *autentizaci (nepopíratelnost),*
- *integritu dokumentu,*
- *funkci ČASOVÉHO RAZÍTKA.*

3.5.2 AUTENTIZACE

Obecně se jedná o proces ověření identity. Pro tento druh procesu se využívají tyto metody:

- *Podle toho, co uživatel zná (heslo, PIN atd.).*
- *Podle toho, co uživatel má (technický prostředek, který uživatel vlastní – privátní klíč, smart card, USB dongle[14]).*
- *Podle toho, čím uživatel je (vlastnosti, které se dají prověřit – otisk prstu, snímek oční zornice apod.).*
- *Podle toho, co uživatel umí (správná odpověď na náhodně vygenerovaný kontrolní odkaz).*

3.5.3 INTEGRITA

Jedná se o stav, kdy přečtená data jsou totožná s daty, která jsou uložena. Zajišťuje kompletnost dat a zachovává data pro jejich zamýšlené použití. Všeobecně můžeme říci, že integrita znamená platnost dat.

Hlavní aspekty:

- *přesnost,*
- *správnost,*
- *platnost.*

Musí splňovat požadavky:

- *Jednoznačné spojení s podepisující osobou.*
- *Umožnění identifikace podepisující osoby ve vztahu k datové zprávě.*

[14] USB dongle – bezdrátový síťový USB adaptér.

- *Vytvoření a připojení k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou kontrolou.*
- *Připojení k datové zprávě takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.*
-

K zajištění integrity slouží tzv. *hashovací funkce*, která vytváří digitální otisk. Proto se také často říká digitálnímu otisku *hash*.

Hash funkce musí zaručovat následující požadavky:

- *Zpráva na vstupu hash funkce má stejnou hodnotu jako kontrolní vzorek.*
- *Nelze provést, aby z výstupního kontrolního vzorku byl zjištěn tvar datové zprávy, ze které byl kontrolní vzorek pomocí hash získán.*
- *Nelze zajistit, aby dvě různé datové zprávy na vstupu hash funkce vedly ke stejnému kontrolnímu vzorku.*

Mezi nejvíce používané hashovací funkce patří algoritmy MD4, MD4 a SHA1. Časově nejstarší je samozřejmě MD4, vytváří 128 bitový digitální otisk. V tomto algoritmu byly však objeveny výrazné slabiny, které tento algoritmus fakticky degradují na 20 bitový. V praxi se s ním už příliš nesetkáme. Vývojovým pokračovatelem tohoto algoritmu je funkce MD5 (Message Digest). Vytváří také 128 bitový digitální otisk, ale není nijak kompromitován. Jako perspektivní se jeví algoritmus SHA-1 (Secure Hash Algorithm). Dokáže vytvořit digitální otisk velikosti 160 bitů, jedná se o standard amerického standardizačního úřadu (NIST). Bezpečnostně ekvivalentní[15] s ním je algoritmus RIPEMD-160.[16]

3.5.4 PROCES VYTVOŘENÍ ELEKTRONICKÉHO PODPISU

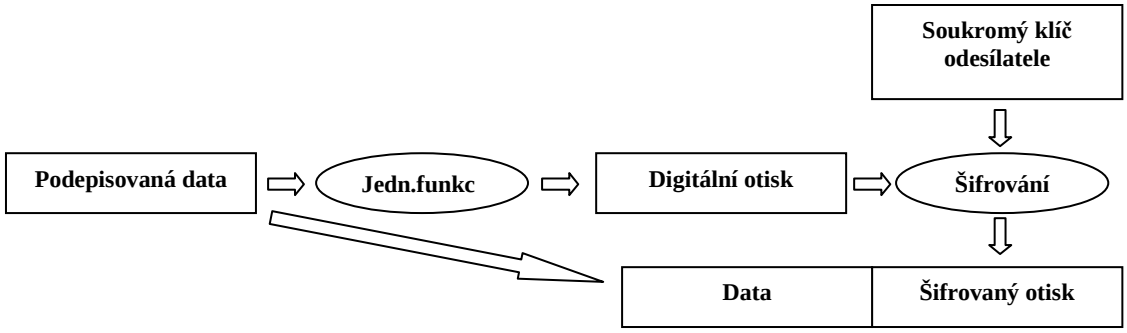
Tento proces je vytvářen ve dvou následujících krocích. Podepisovaná datová zpráva uživatelem, který je vlastníkem privátního klíče a ostatním je znám jeho veřejný klíč, pak z datové zprávy vytvoří pomocí *hash* funkce kontrolní vzorek zprávy. Výstup *hash*

[15] Ekvivalentní – zaměnitelné.

[16] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. Vydání, Brno: Computer Press, 2004. ISBN 80-251-0106-1.

funkce zašifruje PK kryptoalgoritmu a zašifrovaný kontrolní vzorek, tvořící elektronický podpis, ke zprávě připojí.

Obr. A 6: Schéma vytvoření digitálního podpisu[17]

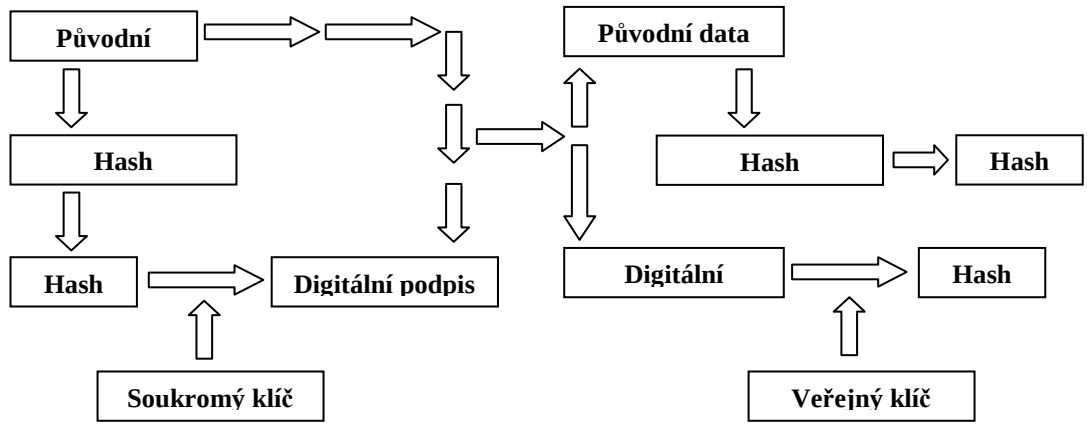


Jsou známy tyto algoritmy:

I) Asymetrické kryptovací algoritmy s veřejným klíčem, nejčastěji RSA (Rivest Shamir-Adleman).

II) Bezpečné kryptografické jednocestné algoritmy (hashovaní funkce), nejčastěji MD5 (Message Digest 5) spolu s RSA a SHA (Secure Hash Algorithm) spolu s DSA.

Obr. A 7: Hashovací funkce.[18]



[17] KRAS, P. *Internet v kostce*. 2. Vydání, Havlíčkův Brod: Fragment, 2002. ISBN 80-7200-510-3.

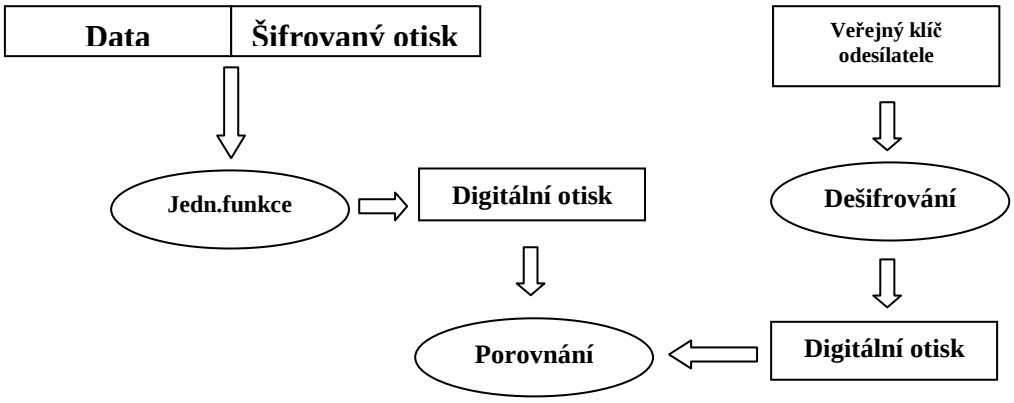
[18] KRAS, P. *Internet v kostce*. 2. Vydání, Havlíčkův Brod: Fragment, 2002. ISBN 80-7200-510-3.

3.5.5 PROCES OVĚŘENÍ ELEKTRONICKÉHO PODPISU

Při ověření elektronického podpisu příjemce se postupuje následovně:

- *Po obdržení datové zprávy elektronickým podpisem vypočte hash funkce kontrolní vzorek zprávy.*
- *S využitím veřejného klíče osoby, která podepsala, dešifruje elektronický podpis a získá kontrolní vzorek zprávy.*
- *Oba zjištěné vzorky porovná a shodují-li se, je pravost elektronického podpisu potvrzena.*

Obr. A 8: Schéma ověření digitálního podpisu.[19]



3.5.6 CERTIFIKAČNÍ LISTINY

Certifikace veřejných klíčů je jedním z nejdůležitějších obraných metod proti infiltraci. Důvěryhodná třetí strana – *Trusted Third Party (Certifikační autorita)* stvrdí svým digitálním podpisem, že konkrétní veřejný klíč patří konkrétní osobě.

Příjemce nejprve ověří podpis v certifikátu, pokud souhlasí, ověří osobní údaje uvedené o odesílateli v certifikátu. Pokud i tyto údaje souhlasí, může přiloženému veřejnému klíči důvěřovat a použít ho k ověření digitálního podpisu vlastní zprávy.

Obdobně jako v bankovnictví, kde se vydávají seznamy ukradených platebních karet, tak i zde vydávají certifikační autority seznamy kompromitovaných klíčů[20]. Jedná se o

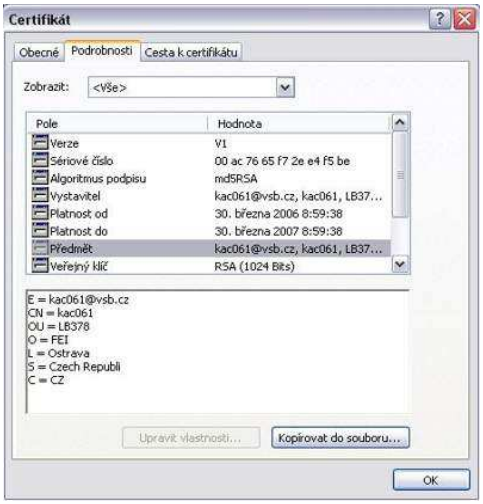
[19] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. Vydání, Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[20] Kompromitace klíčů – zcizení klíčů.

seznam CRL (Certificate Revocation List), v překladu „seznam odvolaných certifikátů“. Příjemce je povinen před vlastním ověřením podpisu zkontrolovat, zda není přiložený certifikát na této černé listině. Pokud tato kontrola nebude vykonána, nese příjemce všechny důsledky slepé důvěry v neplatně podepsaný dokument (obdobným příkladem může být důsledek notářsky neověřeného podpisu na obchodní smlouvě.

Obr. A 9: Certifikát.[21]

Obr. A 10: Obecný popis certifikátu. [22]



Certifikát můžeme označit jako dokument, který stvrzuje, že veřejný klíč (uvedený na certifikátu patří jednoznačně dané osobě. Přesný obsah certifikátu veřejného klíče může

[21] KAČMAŘÍK, Vojtěch. *Výuková podpora předmětu internetové technologie* [online]. [2006] [cit. 2008-05-01]. Dostupný z WWW: <http://homel.vsb.cz/~kac061/>.

[22] KAČMAŘÍK, Vojtěch. *Výuková podpora předmětu internetové technologie* [online]. [2006] [cit. 2008-05-01]. Dostupný z WWW: <http://homel.vsb.cz/~kac061/>.

být obecně libovolný. Existuje však celá řada norem. Nejpoužívanější normou je norma telekomunikační unie – ITU – označována jako X. 509.

Položky certifikátu se rozpadají na 4 logické skupiny:

- *OSOBNÍ ÚDAJE VLASTNÍKA CERTIFIKÁTU (jméno; příjmení; rodné číslo; IČO atd.).*
- *SLUŽEBNÍ ÚDAJE (identifikační číslo; identifikace certifikační autority, které certifikát vydala; informace o použitých algoritmech; splatnost certifikátu atd.).*
- *VEŘEJNÝ CERTIFIKOVANÝ KLÍČ.*
- *DIGITÁLNÍ PODPIS.*

Existují čtyři třídy certifikátů:

- *CLASS 1*

  Certifikační autorita pouze ověří, zda je jméno, které chceme do certifikátu zapsat, je volné.
- *CLASS 2*

  Identita vlastníka certifikátu může být ověřená třetí stranou. K vystavení certifikátu stačí například notářsky ověřený formulář žádosti.
- *CLASS 3*

  Standard mezi certifikáty. Žadatel musí osobně navštívit certifikační autoritu, která předepsaným způsobem ověří jeho totožnost.
- *CLASS 4*

  Podmínky získání tohoto certifikátu jsou stejné jako u předchozí třídy. Přibývá navíc nutnost prokázat oprávněnost vlastníka certifikátu k nějaké činnosti.

3.5.7 CERTIFIKAČNÍ AUTORITA

Jedná se o organizaci, která vydává certifikáty veřejných klíčů. Postupně stále více právních předpisů umožňuje používání certifikátu v oblasti orgánu veřejné správy, to buď při komunikaci mezi úřady navzájem, nebo komunikaci občanů s jednotlivými úřady. Při komunikaci s použitím elektronického podpisu je nutnou podmínkou tzv. *kvalifikovaný certifikát*.

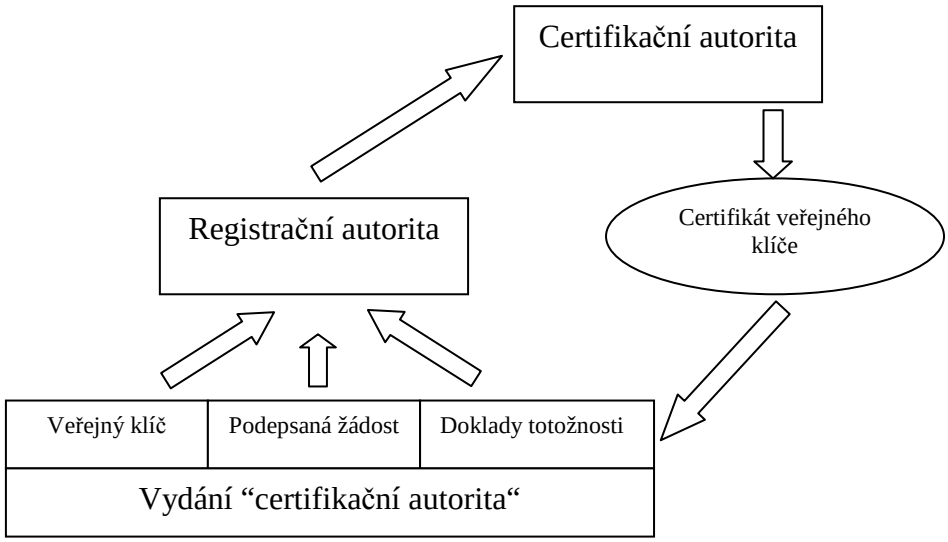
V současné době jsou tři poskytovatelé certifikačních služeb:

- *První certifikační autorita, a. s.*
- *Česká pošta, s. p.*
- *Identity, a. s.*

Certifikační autorita plní dvě základní funkce:

- *Certifikační – zaručující, že deklarovaný veřejný klíč přísluší dané osobě*
- *Validační – potvrzující platnost certifikátu*

Obr. A 11: Princip certifikační autority.[23]



Základním dokumentem certifikační autority je její certifikační politika. Jedná se o veřejně přístupný seznam pravidel, který podrobně popisuje postup při vydávání certifikátů, postup používaný při jejich odvolávání, stanovuje rozsah zodpovědnosti certifikační autority a podobně.

3.5.8 BEZPEČNOST ELEKTRONICKÉHO PODPISU

[23] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. Vydání, Brno: Computer Press, 2004. ISBN 80-251-0106-1.

Ochrana elektronického podpisu se zakládá především na ochraně privátního a veřejného klíče kryptoalgoritmu. A je postavena především na těchto principech:

- *Nemůže dojít k narušení tajnosti privátního klíče.*
- *Není prolomen použitý kryptoalgoritmus ani narušena kryptologická bezpečnost hash funkce.*
- *Nedošlo k porušení autentičnosti veřejného klíče a tím nedodržení záruky, že deklarovaný veřejný klíč přísluší osobě, která zprávu podepisovala.*

Aby byla splněna poslední podmínka, využívá se systém certifikátů, poskytovaných nezávislou třetí stranou – certifikační autoritou (poskytovatelem certifikačních služeb). To vše v případě velkého počtu uživatelů. Pokud jde o malý počet, pak je bezpečnost postavena na vzájemné důvěře. Poskytovatelé certifikačních služeb nejsou nezbytní, ani v případech užívání systému PGP, kdy je autentičnost veřejných klíčů postavena na sdílené důvěře neboli pavučině důvěry.

3.6 OCHRANA DAT

Nebezpečí lze rozdělit na nebezpečí, která hrozí přenášeným datům a ohrožení, která hrozí připojeným počítačům.

Počítačovou síť lze obecně považovat za takzvaný nezabezpečený kanál. Data, která prostřednictvím sítě odesíláme, mohou být s většími či menšími problémy odposlechnuta či dokonce modifikována. Existují také programy, které dokážou odposlouchávat veškerou komunikaci probíhajícím na lokálním ethernetu[24].

Jedná se o velmi nepříjemnou záležitost, neboť o tomto druhu útoku se nemusíme vůbec dovědět. Digitální informace mají takovou vlastnost, že je lze beztrestně kopírovat. Dalším nebezpečím, které z této strany hrozí, je přílišná koncentrace internetových spojení. Ačkoli je internet medium decentralizované, existuje poměrně malý počet míst, přes která proudí poměrně velké množství dat. Pokud útočník získá kontrolu nad tímto místem, případně pokud je útočník přímo správce tohoto bodu, potom má možnost kontroly nad velkou částí dat přenášených přes internet.

[24] Ethernet – je typem lokální sítě, který realizuje vrstvu síťového rozhraní. Jeho předností je jednoduchý protokol, snadná implementace a instalace.

Při útoku na připojený počítač nejprve útočník zjišťuje, které síťové služby na počítač pracují. Většina služeb má pevně předdefinované porty, na kterých musí odpovídat na výzvu klienta či serveru protistrany (např. u FTP se jedná o port 21). Jakmile je na tento port zaslána zpráva, musí FTP server odpovědět předepsaným způsobem. V průběhu prověřování portů získá útočník mnoho údajů o protokolech a programech, které jsou na daném počítači spuštěny. Útočník může vyzkoušet *slovníkový útok na protokoly*, které vyžadují heslo. Například u již zmíněného FTP serveru zvolí vhodné jméno. Posléze zkouší použít jako heslo některé z tisíců slov, které má uložená ve slovníku. Řada lidí si totiž jako heslo volí slovo ve svém jazyce.

Útočník musí v každém případě získat nad počítačem alespoň částečnou kontrolu. Pokud to zamýšlí, kontrola mu umožní právě již zmiňovaný odposlech nebo modifikace dat. Nepodaří-li se získat kontrolu, zbývá ještě stále jeden druh útoku - *útok na dostupnost počítače.*

Tento druh útoku je specifický tím, že je počítač přehlcen opakovanými či nesmyslnými dotazy, díky čemu nestíhá reagovat na regulérní dotazy jiných počítačů. Tento útok nese označení Denial of Service – DoS (odepření služby). Protože je však zahlcení výkonného serveru z jednoho PC prakticky nemožné, využívají útočníci postupu, kdy nejprve získají kontrolu nad velkým množstvím počítačů kdekoliv na internetu a v daném momentě dají pokyn k zahlcení jednoho serveru. Tento útok se označuje jako *Distributed DoS – DdoS.*

3.6.1 KOMUNIKAČNÍ PROTOKOLY

Pro přenos dat prostřednictvím počítačové sítě se používají takzvané komunikační protokoly. Jiné protokoly se pak používají pro odesílání a přijímání elektronické pošty, zcela jiný zase pro přenos souborů, stahování internetových stránek a podobně.

Rozlišujeme tyto protokoly:

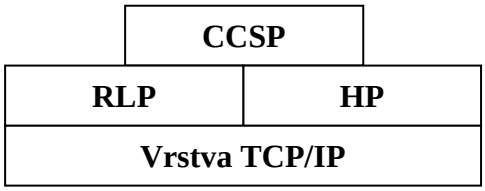
- *Telnet Protocol.*
- *SSH Protocol (transport layer protocol, authentication protocol, connection protocol)*
- *FTP – File, Transfer Protocol.*
- *Secure FTP.*

- *HTTP – Hyper Text Transfer Protocol (rekord layer protocol, handshake protocol, change cipher specification protocol, alert protocol, SSL protocol).*

3.6.2 PROTOKOL SSL

Protokol SSL je zajímavý tím, jakým způsobem jsou ustanoveny klíče pro šifrování přenášených dat. Klient i server mají stejný vliv na jejich výslednou podobu.
Komunikace je odstartována zasláním certifikátu veřejného klíče serveru. Klient vygeneruje náhodné číslo, zašifruje ho obdrženým veřejným klíčem a zašle serveru zpět. Toto číslo je označováno jako *premaster secret*. Z náhodných čísel vyměněných při předchozí komunikaci a *premaster secret* je vytvořeno *master secret*. Obě strany vygenerují a vymění si náhodná čísla. Z *master secret* a vyměněných náhodných čísel si každá strana vytvoří materiál pro tvorbu klíče. Vlastní klíč je tvořen vybranými bity z tohoto materiálu.

Obr. A 12: Struktura protokolu SSL.[25]



Protokol SSL dokáže přebírat a šifrovat data od jakéhokoliv protokolu, nejen od protokolu HTTP. Tento protokol lze využít i pro ochranu elektronické pošty.
V tomto momentě se ale jedná o ochranu komunikace mezi klientem a serverem, případně mezi dvěma servery. Ustanovit SSL spojení mezi dvěma koncovými uživateli je prakticky nemožné. Odeslaná data jsou zašifrovaná, předána poštovnímu serveru, který je dešifruje. Následně data putují k poštovnímu serveru příjemce, i tento přenos může být chráněn pomocí protokolu SSL, koncový poštovní server je opět dešifruje. Konečná část přenosu probíhá mezi adresátovým poštovním serverem a adresátem.

[25] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. Vydání, Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

3.6.3 FIREWALLY

Obecně lze říci, že útok na zabezpečenou síť může být veden odkudkoliv a jakýmkoliv způsobem. *Základní pravidlo obrany* – uživatelé musí mít povoleno naprosto nezbytné minimum činností, vše zakážeme a povolujeme jen to, co je bezpodmínečně potřeba povolit.
Prvním krokem k obraně sítě před útokem z vnějšku je centralizace propojená s vnějším světem. Samotná centralizace přípojných bodů k ochraně sítě nepostačuje, i její zajištění však často bývá nemalý problém.Pro tuto funkci využívá správně nakonfigurovaný firewall.

3.6.4 ROZDĚLENÍ FIREWALLŮ

Firewall je sada opatření (hardwarových, softwarových či personálních), která mají za cíl propojit dvě nebo více sítí s různou úrovní důvěryhodnosti tak, že sníží rizika vyplývajících pro chráněné sítě z tohoto propojení.
Základní technologie používané při tvorbě firewallů můžeme rozdělit do několika skupin. Firewall není čistě teoretická záležitost, různě tedy kombinuje několik popsaných technik. Může být jak softwarový program běžící na vyhrazeném počítači, tak hardwarové zařízení zapojené mezi chráněnou sítí a internetem.

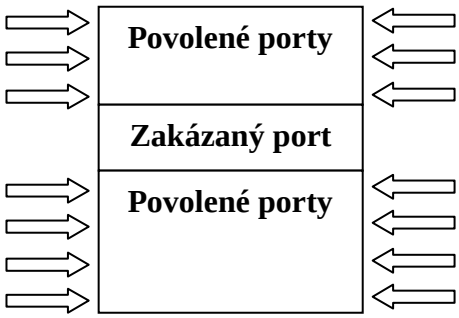
Základní technologie:

- Jednoduchý IP filtr.
- Stavový IP filtr.
- Proxy.

3.6.5 JEDNODUCHÝ FILTR

Funguje jako blokovač internetového provozu. Pracuje podle sady pravidel, které zakazují provoz na jednotlivých portech. Veškerý nezakázaný provoz je povolený. Nevýhoda spočívá v tom, že abychom ošetřili všechna možná nebezpečí, musíme zakázat celou řadu portů.

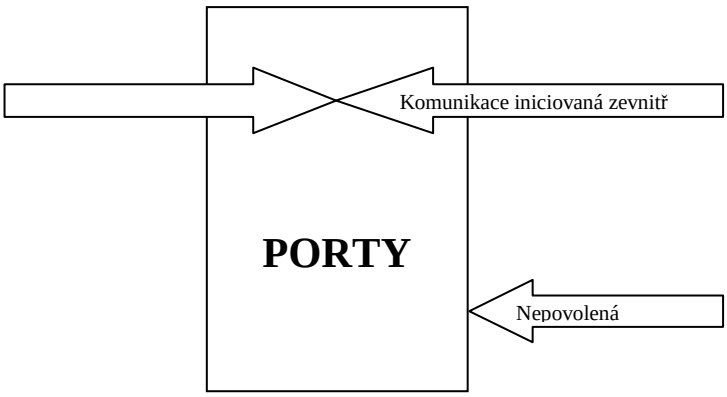
Obr. A 13: Jednoduchý IP filtr. [26]



3.6.6 STAVOVÝ FILTR

V jádře je uchována tabulka stavů, filtr monitoruje síťový provoz a upravuje podle něj tabulku stavů. Následně ho povoluje či zakazuje podle nastavených pravidel a stavové tabulky. Díky tomu má sice omezenou, ale přece jen nějakou možnost kontroly podle aplikační vrstvy.

Obr. A 14: Stavový filtr.[27]



[26] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. Vydání, Brno: Computer Press, 2004. ISBN 80-251-0106-1.

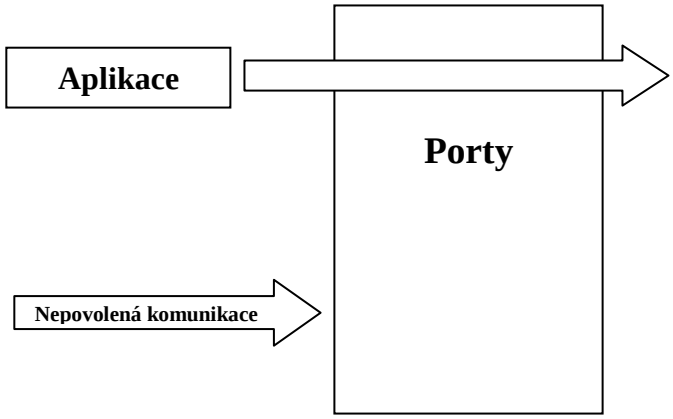
[27] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. Vydání, Brno: Computer Press, 2004. ISBN 80-251-0106-1.

Filtr sleduje komunikaci protokolů vyšší vrstvy, především TCP[28] a UDP[29]. Povolí jakýkoliv průchod paketů z vnitrofiremní sítě směrem do internetu. Opačně pak povolí jen ty pakety, které patří k nějaké zevnitř vyprovokované relaci.

3.6.7 PROXY

Nejpokročilejší, avšak také hardwarově nejnáročnější technologií používanou při tvorbě firewallů, je *aplikační proxy*. Jedná se o program určený pro jeden konkrétní protokol, který filtruje pakety podle toho, která aplikace a na kterém portu s nimi pracuje. V praxi tak může mít jeden program přístup například k portu 110 (POP3 – stahování pošty), zatímco pro ostatní programy je tento port "tabu".

Obr. A 15: Aplikační proxy.[30]



Původně bylo nutno před zahájením relace sdělit bráně, s kým a pomocí jakého protokolu chce uživatelův program komunikovat. Moderní proxy brány jsou dostatečně

[28] TCP (Transmission Control Protocol) – představuje transportní vrstvu, kdy s jeho pomocí mohou aplikace na počítačích propojených do sítě vytvořit mezi sebou spojení, přes které se mohou přenášet data.

[29] UDP (User Datagram Protocol) – protokol, který je vhodný pro nasazení, kde je vyžadována jednoduchost nebo pro aplikace pracující systémem otázka-odpověď (např. DNS, sdílení souborů v LAN).

[30] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. Vydání, Brno: Computer Press, 2004. ISBN 80-251-0106-1.

transparentní, uživatel a jeho programy nemusí o existenci takové brány vůbec vědět. Kvalitní brány také slouží pro filtraci více protokolů současně.
Filtrovány jsou všechny pakety, jejichž propuštění není explicitně povoleno, což je zásadní rozdíl oproti IP filtrům, přináší to celou řadu výhod. Především rychlejší konfiguraci a vyšší úroveň bezpečnosti. Nedostatkem je zde horší přizpůsobivost k novým protokolům.

Ostatní vnitřní síť je s internetem propojena pomocí normálního firewallu. Výsledkem je tedy ještě větší zabezpečenost zbytku sítě (proto se oblast, která je chráněna sice dostatečně, ale jiným způsobem, nazývá demilitarizovaná zóna).

3.6.8 PERSONÁLNÍ FIREWALLY

V zásadě se jedná o jistou obdobu instalace antivirových systémů na pracovní stanice. Jeden antivirus sice kontroluje veškerou příchozí i odchozí poštu, antivirus na stanicích má úlohu kontroly stahovaných souborů a souborů přenesených pomocí fyzických nosičů (CD disky, diskety, flash disk apod.).

Umístění firewallu na cílovém počítači poskytuje několik výhod:

- *Delší analýzy přenášených dat.*
- *Konfigurace podle požadavků uživatele.*
- *Nezměněná funkčnost mimo firemní síť.*

4. ANALÝZA PROBLÉMU A SOUČASNÝ STAV ŘEŠENÉ PROBLEMATIKY

Pro analýzu elektronického (digitálního) podpisu jsem si pro vybral státní útvar. *Ministerstvo financí ČR.*

V poslední době je čím dál více rozvíjena elektronická komunikace mezi úřady a klienty, především v sektoru financí elektronická komunikace prakticky už nahradila ústní. A to především zasílání dokumentů v digitální podobě místo zdlouhavého

zpracování dokumentů v tištěné podobě. Samozřejmostí u elektronických dokumentů je digitální podpis nebo zaručený digitální podpis.

4.1 POPIS ANALYZOVANÉHO SUBJEKTU

Název subjektu: Ministerstvo financí České republiky

Ministerstvo bylo jako ústřední orgán státní správy zřízeno zákonem ČNR č.2/1969 Sb., o zřízení ministerstev a jiných úředních orgánů státní správy České republiky, ve znění pozdějších předpisů (dále jen „kompetenční zákon“) – viz jeho 1 § bod 1. Organizační struktura ministerstva k 31. 12. 2006 je Přílohou č. 1 Roční zprávy.

Předmět činností subjektu

Jedná se o státní závěrečný účet, státní pokladnu, finanční trh a ochrana zájmů spotřebitelů na finančním trhu s výjimkou dohledu nad kapitálovým trhem v rozsahu působnosti České národní banky, daně, poplatky a clo, finanční hospodaření, finanční kontrola, přezkoumávání hospodaření USC, účetnictví, audit a daňové poradenství, věci devizové včetně pohledávek a závazků státu vůči zahraničí, ochrana zahraničních investic, tombol, loterie a jiné podobné hry, hospodaření s majetkem státu, privatizace majetku státu, příspěvek ke stavebnímu spoření a státní příspěvek na penzijní připojištění, ceny, činnost zaměření proti legalizaci výnosů z trestné činnosti, posuzovaní dovozu subvencovaných výrobků včetně opatření na obranu proti dovozu těchto výrobků, zajišťovaní členství v mezinárodních hospodářských seskupeních, koordinace příjmů zahraniční pomoci.

Zpracovává koncepce rozvoje svěřeného odvětví a pečuje o náležitou právní úpravu, včetně přípravy návrhu zákonů a jiných právních předpisů. Zabezpečuje v oblasti své působnosti mezinárodně smluvní agendu, mezistátní styky a mezinárodní spolupráci, plní úkoly vyplývajícího pro ČR z mezinárodních smluv a z členství v mezinárodních organizacích.

4.2 ELEKTRONICKÉ PODÁNÍ (EPO)

Ministerstvo financí umožnilo subjektům podávat daňové přiznání a další písemnosti v elektronické podobě. Podání lze uskutečnit prostřednictvím sítě Internet nebo také pomocí fyzických nosičů (disketa atd.). Podání po Internetu lze uskutečnit dvěma odlišnými způsoby;

I) *Podání datovou zprávou opatřenou zaručeným elektronickým podpisem.*

II) *Podání datovou zprávou neopatřenou zaručeným elektronickým podpisem (při této možnosti je ještě vyžadováno podání v písemné podobě, tj. doručení počítačové sestavy správci daně neboli e-tiskopis).*

Řešení vychází zejména z ustanovení zákona č.337/1992 Sb., o správě daní a poplatků, ve zněná pozdějších předpisů a dalších předpisů. Aby byla zachována autentičnost údajů na technickém nosiči dat a v písemnosti (v případě datové zprávy neopatřené zaručeným elektronickým podpisem), musí být obojí opatřeno kontrolním údajem – číslem, jehož správnost je při příjmu na příslušném finančním úřadu kontrolována. Kontrola písemnosti a doplňování uvedených kontrolních informací jsou jedním z hlavních funkcí této aplikace.

Aplikaci je možné použít třemi metodami:

I) Písemnost v souboru, připraveném ve stanovené struktuře v nabídce Technická specifikace – STRUKTURY VSTUPNÍCH SOUBORŮ (z databáze nebo např. účetního SW) je pomocí funkcí v části PÍSEMNOSTI V SOUBORU zkontrolována, opatřena kontrolními čísly, uložena, případně odeslána na místě na příslušný finanční úřad.

II) Pro písemnosti dle nabídky je možné připravit novou písemnost v elektronické podobě pomocí "inteligentního" elektronického formuláře v nabídce PODÁNÍ.

III) Písemnost souboru je vytvořena a odeslána na příslušný finanční úřad přímo z používané aplikace (účetní, daňový SW).

4.2.1 ROZHRANÍ

Aplikačním rozhraním je zde míněna struktura vstupních parametrů, přístupových bodů a výstupních informací, které je možné používat pro zpracování a ze kterých je možné získávat informace vztahující se k písemnosti. Rozhraní je připraveno tak, aby mohlo být používáno výrobci aplikačního vybavení (např. účetnictví) ke zpracování a odeslání písemnosti z aplikace.

Rozhraní se člení do tří částí:

I) *Číselníky – slouží pro získávání koeficientů používaných při kontrolách písemnosti, pro před vyplnění položek a pro vytváření výčtových nabídek.*
II) *Příjem písemnosti (podání) – je určena pro příjem souboru na sever MF, odkud je pak doručen na příslušný finanční úřad.*
III) *Stav podání – zjišťuje stav odeslaných (podání).*

4.2.2 ROZHRANÍ ČÍSELNÍKŮ

Toto rozhraní číselníků je ovládáno pomocí URL parametrických řádků. Struktura číselníků je ve formátu XML. Ve výsledku výběru může být žádný, jeden nebo množina záznamů.

Vyhledávání je prováděno dvojím způsobem:

I) Hledáním podle určitého klíče (resp. určitých klíčů) pomocí specifikace Xpath.
II) Hledáním nejbližší hodnoty v určitém intervalu.

Pro posílání dotazů na číselníky platí ještě další pravidla. Tím pravidlem je formát dotazu v UTF-8, který je navíc ještě kódován podle specifikace URL[31].

[31] URL (Uniform Resource Locator) – jedná se o řetězec znaků s definovanou strukturou, který slouží k přesné specifikaci umístěných zdrojů informací na Internetu.

Tab. 1: Parametry volání.[32]

PARAMETR	NÁZEV	S PARAMETRY	POPIS
C	číselník	XP,PL,T	Výběr číselníku, kterému se výběr vztahuje (viz. Seznam).
XP	Xpath	C,PL,T	Specifikace vyhledávacích parametrů podle standardu Xpath.
PL	platnost	C, XP, PL,T, K, H	Formát parametru RRRR-MM-DD.
K	klíč intervalu	C, PL, H, K	Vícenásobný parametr specifikující klíče pro vyhledávání intervalu.
H	hodnota intervalu	C,PL,K	Parametr specifikuje číselnou hodnotu klíče uvedeného jako první parametr K, pro který je hledána nejbližší hodnota v intervalu.
T	třídění	C,PL,XP	Specifikace třídění výsledné množiny, parametr obsahuje dva znaky pro třídění: 1. znak typ třídění T-textové, N-numerické 2. znak způsob S-sestupně, V-vzestupně a dále podtržítko a název atributu včetně znaku "@". Např.: &T=NV_@paragraf

4.2.3 PODÁNÍ PÍSEMNOSTI

V této části je obsažena hlavní funkce přijmu písemnosti (podání) do daňové správy.
Ovládání rozhraní je založeno na kombinaci parametrických řádků a odesílání neformátovaných dat metodou POST (RFC 2616): - parametrické řádce může být jako parametr“&email=…….“ uveden email, na který mají být posílány informace o změně stavu podání. Obsah zasílaných neformátovaných dat musí odpovídat struktuře písemnosti ve formátu XML. Pokud je podání posíláno se zaručeným elektronickým podpisem (ZAREP), musí být struktura “zabalena“ do příslušného formátu kryptografických struktur.
Soubor, který je úspěšně podroben kontrole a uložení, je zpět vráceno tzv. potvrzené podání – jedná se o soubor ve formátu PKC #, podepsaný elektronickým podpisem (nekvalifikovaným) certifikátem podatelny – *Společného technického zařízení správců daně.*

[32] *MF: Elektronické zpracování písemnosti* [online]. 1999-2006 [cit. 2008-05-01]. Dostupný z WWW: http://adisepo.mfcr.cz/adis/jepo/.

Tab. 2: XML struktura potvrzení písemnosti.[33]

ELEMENT/ATRIBUT	NÁZEV	POPIS
Písemnost	Hlavní element písemnosti	Uzavírající element určující, že se jedná o písemnost.
Písemnost/Data	Kopie původního podání	Obsahuje data v hexadecimální kódování odeslané písemnosti.
Písemnost/Kontrola	Kontrolní element aplikace	Obsahuje kontrolní položky pro podání a pro aplikaci.
Písemnost/Podání	Element informací o podání	Obsahuje atributy s informacemi o učiněném podání.
Písemnost/ Podaní/ Číslo	**Podací číslo**	**Referenční údaj.**
Písemnost/ Podaní/ KC	Kontrolní číslo podání	Údaj, který se nepoužívá. Je uveden z důvodu zpětné kompatibility.
Písemnost/ Podáni/ Datum	**Datum a čas podání**	**Datum a čas jsou ve standardním formátu XML dle normy.**
Písemnost/ Podáni/ Heslo	**Heslo pro přístup k inf. o podání**	**Heslo přidělené systémem.**
Písemnost/ Podáni/ ZAREP	true/false	Indikátor určující ZAREP v podané písemnosti.
Písemnost/ Podáni /e-mail	Notifikační e-mail , adresa	Slouží k zasílání informací o stavu zpracování podání.

Testovací režim

Připravená data je možné na server poslat pouze k otestování, a to pomocí parametru "&test=1". Podání bude otestováno (ZAREP, formální i věcné kontroly a obsahu), ale nebude podáno. Vrací se pouze XML dokument všech zjištěných chyb.

Kódování

Soubory CML, které jsou přijímány v centrální podatelnou, musí být kódovány. XML zpráva elektronické potvrzenky je vydávána vždy v kódování UTF-8.

4.2.4 ZJIŠTĚNÍ STAVU PODÁNÍ

Je zárodkem pro elektronické nahlížení do spisu. Umožňuje zjišťování stavu odeslané písemnosti (podmínkou je známé podací číslo a vygenerované heslo).

Rozlišujeme:

- *C=….. Existující podací číslo.*

[33] *MF: Elektronické zpracování písemnosti* [online]. 1999-2006 [cit. 2008-05-01]. Dostupný z WWW: http://adisepo.mfcr.cz/adis/jepo/.

- *H=….. Heslo vztahující se k zadanému číslu.*

Zde je struktura ve formátu XML obsahující hlavní element <Stav/> a podelementy (textové) s požadovanými informacemi.

Tab. 3: Struktura informací ve formátu XML.[34]

ELEMENT	NÁZEV	HODNOTY	POPIS
pro_podani	Podací číslo	číslo	Identifikátor písemností
apl_oblpod	Aplikační oblast	3 znaky	Odpovídá první části zkratky označení písemnosti.
typ_podani	Typ podání	3 znaky	Vyjadřuje typ písemnosti.
c_ufo_prij	Číslo cílového finančního úřadu	Číslo 1 až 499	Odpovídá číslu finančního úřadu.
e-mail_ext	E-mail	255 znaků	
d_podani	Datum odeslání	datum	Datum uložení písemnosti do centrální databáze MF.
cas_podani	Čas odeslání	čas	Čas uložení písemnosti do centrální databáze MF.
p_zareppod	Příznak podání se ZAREP	1 znak	Hodnoty: A - podání se ZAREP N - podání bez ZAREP.
p_platnostpod	Platnosti ZAREP	1 znak	Hodnoty: A - platný podpis N - neplatný podpis C - obsahuje chyby K - opožděná kontrola platnosti.
p_chybapod	Příznak chyby dat podání	1 znak	Hodnoty: N - data bez chyb S - chyba struktury v datech podání K -kritická chyba I - chyba informací.
stav_podpre	Stav podání MF	číslo 0 - 5	Stav podání v centrálním úložišti na serveru MF.
stav_podpre_text	Popis stavu podání MF	255 znaků	Hodnoty: 0 - uloženo /opožděná kontrola platnosti podpisu 1 - uloženo/ bez kontroly opožděné platnosti podpisu 2 - podání na FÚ 3 - doručení na FÚ (doručenka o uložení do databáze) 4 - potvrzení o doručení na FÚ zasláno poštou dodavateli 5 - potvrzení o přijetí či odmítnutí na finančním úřadu zasláno poštou podavateli.
stav_podapl	Stav podání FÚ	číslo 1 - 3	Stav zpracování podání na finanční úřad.
stav_poddapl_text	Popis stavu podání FÚ	255 znaků	Hodnoty: 1 - podání nebylo zpracováno 2 - podání bylo odmítnuto 3 - podání bylo přijato.
d_pripodapl	Datum zpracování FÚ	datum	Datum zpracování písemnosti.
pozn_pripodapl	Poznámka zpracování aplikací	255 znaků	V případě odmítnutí - obsahuje text poznámky, krátké odůvodnění.

Toto rozhraní je ovládáno pomocí parametrů odesílaných metodou HTTP POST (RFC 2616).

[34] *MF: Elektronické zpracování písemnosti* [online]. 1999-2006 [cit. 2008-05-01]. Dostupný z WWW: http://adisepo.mfcr.cz/adis/jepo/.

4.2.5 ZARUČENÝ PODPIS (ZAREP)

Datové zprávy opatřené zaručeným elektronickým podpisem, které přijímá *Společenské technické zařízení správců daně,* musí být vytvořeny ve formátu *PKC S #7 verze 1.5 (RFC 2315)*. PKCS #7 objekt musí být ve formátu *DER (ITU-T Recommendation X. 690).*

Obsah PKSC #7 objektu datové zprávy opatřené zaručeným elektronickým podpisem, musí splňovat následující podmínky:

- *Musí být typu „signedData“.*
- *Musí obsahovat podepisovaná data (není přípustná reference).*
- *Musí obsahovat certifikát podepisujícího.*
- *Musí obsahovat právě jeden elektronický podpis.*

Kontrola zprávy se zaručeným e-podpisem je prováděna pomocí kryptografických kontrol. Kontroluje se také certifikát podepisujícího, který musí být vydán akreditovaným poskytovatelem certifikačních služeb a musí obsahovat bezvýznamný identifikátor klienta MPSV.

4.2.6 SYSTEMOVÉ POŽADAVKY

Přístup k jednotlivým částem aplikace EPO pro elektronická podání daňových přiznání se na prohlížeče liší. Úvodní stránky se všemi informacemi a popisy povoluje jakýkoli prohlížeč pracující s HTML4 (podporujícím rámy (frames)). Zpracování datového souboru a kontroly podání, včetně volitelného podepsání zaručeným elektronickým podpisem a odeslání na Společné technické zařízení správců daně, je možné v Internet Exploreru nebo v jiných alternativních prohlížečích.

Podporované prohlížeče:

- *Internet Explorer 6 Service Pack 1 a vyšší*
- *Mozilla 1.6 a vyšší*
- *Firefox 0.8 a vyšší*
- *Netscape 7 a vyšší*

Pro vyplňování daňových formulářů i odeslání datové zprávy je vyžadována SUN Java. Podporovaná je verze SUN 1.5 a vyšší.

Mezi podporované operační systémy této aplikace patří:

- *Microsoft Windows 2000*
- *Microsoft Windows XP*
- *Knoppix verze 3.6 (Debian Linux)*

Pro vytvoření zaručeného elektronického podpisu k odesílanému datovému souboru je potřeba mít soukromý klíč, ke kterému byl vydán akreditovaným poskytovatelem certifikačních služeb kvalifikovaný certifikát dle zákona 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů. Pro jednoznačnou identifikaci osoby se používá tzv. bezvýznamný identifikátor 1MPSV.

4.2.7 BEZPEČNOST

Zabezpečení aplikace je postaveno v souladu s ustanoveními zákona č.337/1992 Sb. o správě daní a poplatků, ve znění pozdějších předpisů a zvláštních daňových zákonů.

Zabezpečení lze rozdělit tří základních oblastí:

I) Vlastní důvěryhodnost aplikace.
II) Zpracování písemnosti včetně doručení.
III) Příjem písemnosti a její zpracování včetně informací o stavu zpracování.

Vlastní důvěryhodnost aplikace

Přístup k aplikaci je pomocí nezabezpečeného HTTP protokolu (adresa začínající http:). Aplikaci lze ovšem použít také pomocí chráněného (šifrovaného) kanálu protokolem HTTPS (stačí v položce adresy zaměnit http: za https), které je ale pomalejší. V daném protokolu začíná spojení prokázáním totožnosti serveru, na kterém je stránka umístěna.
Aplikační kód, jež má na starost zpracování písemnosti a její kontrolu, je ochraňován proti zneužití tzv. podpisem vydavatele. Vlastník aplikace (MFČR) zaručuje, že aplikace neprovede žádnou operaci, která by mohla uživatele poškodit. To se projeví zobrazením certifikátu vydavatele při načtení knihoven po vstupu do formuláře nebo kontrolního programu pro vstup souboru.

Zpracování písemnosti a její doručení

Z důvodů ochrany osobních dat uživatele je celé zpracování písemnosti prováděno na jeho počítači a žádná její část není nikde jinde umisťována.

Písemnost pak může být odeslána na příslušný úřad pomocí sítě Internet, zatímco aplikace může být načtena pomocí chráněného i nechráněného protokolu HTTP. Komunikace pak probíhá pomocí již zmiňovaného kanálu SSL, který provádí šifrování odesílaných dat na straně uživatele pro příjemce (Společné technické zařízení správců daně). Server je umístěný v chráněném prostoru Ministerstva financí ČR, který je od sítě Internet oddělen technickými prostředky (firewall), což vylučuje možnost úprav písemnosti třetí stranou kdekoliv mezi počítačem daňového subjektu a serverem.

Ze společného serveru je písemnost přenášena na příslušný finanční úřad, kde je pak dále zpracovávána obdobně jako běžná písemnost do elektronické podoby.

Příjem písemnosti a stav zpracování

Na finančním úřadě je písemnost přístupná pouze správci daně. O změně stavu písemnosti (její doručení na finanční úřad, přijetí/odmítnutí atd.) může být daňový subjekt také informován elektronicky (e-mail). Pro zaručení bezpečnosti informací je v elektronické zprávě pouze indikace změny stavu písemností bez dalších informací a uživatel může zjistit stav zpracování písemností přímým přístupem na stránku o stavu s tím, že musí zadat podací číslo písemnosti a heslo zobrazené po odeslání písemnosti. I tato komunikace probíhá prostřednictvím kanálu SSL.

4.2.8 POPIS STRUKTURY SOUBORU

Společnou vlastností všech elektronických podání je jejich platforma (předepsaný obsah).

Vstupní soubor může být ve **formátu XML** nebo ve formátu se záznamy oddělenými **pomocí oddělovačů**, resp. s pevnou délkou záznamu.

V existujících e-podáních pro příjem souboru s oddělovači byla struktura organizována do vět skládajících se z položek. Tato podoba je v základu zachována i ve struktuře XML předávaných informací.

Pravidla:

Základem je *POLOŽKA* v písemnosti:

- *Ta je popisována určitými pravidly, která charakterizují její, typ, rozsah, nebo vymezují hodnoty, jakých může nabývat.*

Položky jsou seřazeny do *VĚT*:

- *Každá věta je popsána svým názvem, typem a atributy definující její výskyt v písemnosti.*

Věty definují vlastní *PÍSEMNOST:*

- *Charakterizovanou jednoznačným názvem a verzí.*

Pro úplnost definice písemnosti zde patří také kontrolní parametry nahrazující elektronické podpisy aplikace, daňového subjektu, podatelny. Kromě vět mohou být v písemnosti také přílohy.

Soubor vstupující do aplikace může mít jakýkoliv název a aplikace sama rozezná jeho typ a písemnost, ke které se vztahuje. Pojmenování výstupních souborů je podle platných pravidel pro označování elektronických písemností, aby nemohlo dojít k záměně při příjmu na podatelně finančního úřadu (zaručeno vložením základní identifikace a data).

4.2.9 SPECIFIKACE STRUKTURY SOUBORU

Tab. 4: Struktura vět.[35]

TYP	POPIS	MIN.POČET	MAX.POČET	POLOŽKY
D	Bez popisu	1	1	k_uladis, dokument, misto, d_vyhotov,
P	Bez popisu	0	1	c_ufo, dic, rod_c, typ_ds, prijmeni, jmeno,titul, zkrobchjm, naz_obce, c_obce,ulice, c_pop, c_orient, psc, stat, k_stat, opr_prijmeni, opr_jmeno, opr_titul, opr_naz_obce,opr_c_obce, opr_ulice, opr_c_pop, opr_c_orient,opr_psc, opr_postaveni, opr_rod_c, opr_d_nar,opr_k_stat,

[35] *MF: Elektronické zpracování písemnosti* [online]. 1999-2006 [cit. 2008-05-01]. Dostupný z WWW: http://adisepo.mfcr.cz/adis/jepo/.

Věta D

ZKRATKA	TYP POLOŽKY	DÉLKA	ČÍSLO	PŘÍPUSTNÉ HODNOTY	POPIS
c_ufo	Číslo	3			**Finanční úřad** (místně příslušného správce daně)
dic	Číslo	10			**DIČ**
rod_c	Číslo	10			**Rodné číslo**
typ_ds	Text	1		P, F	**Typ daňového subjektu**
prijmeni	Text	36			**Příjmení**
jmeno	Text	20			**Jméno**
titul	Text	10			**Titul**
zkrobchjm	Text	255			**Obchodní firma / název**
naz_obce	Text	48			**Obec**
c_obce	Číslo	6			**Číslo obce**
ulice	Text	38			**Ulice**
c_pop	Číslo	6			**Číslo popisné**
c_orient	Text	4			**Číslo orientační**
psc	Číslo	5			**PSČ**
stat	Text	25			**Stát**
k_stat	Text	2			**Kód státu**
opr_prijmeni	Text	36			**Příjmení (jednatele)**
opr_jmeno	Text	20			**Jméno (jednatele)**
opr_titul	Text	10			**Titul (jednatele)**
opr_naz_obce	Text	48			**Obec**
opr_c_obce	Číslo	6			**Číslo obce**
opr_ulice	Text	38			**Ulice**
opr_c_pop	Číslo	6			**Číslo popisné**
opr_c_orient	Text	4			**Číslo orientační**
opr_psc	Číslo	5			**PSČ**
opr_postaveni	Text	40			**Postavení k subjektu**
opr_rod_c	Číslo	10			**Rodné číslo**
opr_d_nar	Datum	10			**Datum narození**
opr_k_stat	Text	2			**Stát**

Věta P

ZKRATKA	TYP POLOŽKY	DÉLKA	ČÍSLO	PŘÍPUSTNÉ HODNOTY	POPIS
k_uladis	Text	3		DPR	**Daňový portál** - písemnosti pro daňový portál
dokument	Text	3		ZA1	**Žádost o zřízení daňové informační schránky** - touto písemností žádá subjekt podle §34 ods. 2 zákona č.337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů, o zřízení daňové informační schránky.
místo	Text	20			**Místo vyhotovení** - používá se v záhlaví úplného opisu pro určení místa " V ….. dne ……".
d_vyhotovení	Datum	10			**Datum vyhotovení** - používá se v záhlaví úplného opisu pro určení data " V ….. dne ……".

4.2.10 FORMÁT SOUBORU XML

Pro vytváření XML dokumentů platí základní pravidla tvorby XML dokumentů podle organizace W3C „Extensible Markup Language (XML) 1.0 (Second Edition) http*://www.w3.org/TR/REC-xml*“, včetně kódování národní ZNAKOVÉ SADY (pro české znaky lze brát v úvahu pouze kódování WINDOWS-1250, ISO-8859-2 a univerzální UTF-8,resp. UTF-16).
Základní struktura se skládá z ***VĚT*** a ***POLOŽEK***. Jelikož se položky (v rámci věty) nemohou opakovat, jsou v souboru jako ***ATRIBUTY*** věty. Věty umožňující opakování tvoří ***ELEMENTY*** vlastní písemnosti.

Písemnost ve formátu XML má jako hlavní (root) element
<***Pisemnost***>
……
</***Pisemnost***>
V elementu písemnosti se nachází element odpovídající typu písemnosti, např.:
<***DSLDAP***>
……
</***DSLDAP***>
a v něm se nachází věty souboru podle popisu struktury. Každý element věty začíná slovem „Veta“ doplněné o písmeno typu věty, např.:
<***VetaP…/***>
Věta obsahuje atributy nesoucí hodnoty, jejichž název odpovídá názvům položek příslušné věty, např.:
<***VetaP jmeno=“Pavel“ kc_danpo=“200“/***>

V elementu výstupní písemnosti se nachází ještě element obsahující kontrolní informace:
<***Kontrola***>
…...
</***Kontrola***>

Struktura souborů je popsána a při příjmu také kontrolována pomocí tzv. XML schémat, a to podle specifikace: *W3C XML Schema.*

4.2.11 FORMÁT SOUBORU S ODDĚLOVAČI

I když je preferovanou formou XML, lze také vytvářet vstupní soubor s oddělovači záznamu. Zásady vytváření vstupního (zdrojového) souboru v tomto formátu jsou:

I) Jeden vstupní datový soubor = údaje pro jednu písemnost jednoho subjektu.

II) Ve vstupním datovém souboru je nutno dodržovat stanovené pořadí jednotlivých položek.

III) Desetinná čísla mají jako oddělovač čárku.

IV) Kódování českých znaku WINDOWS-1250.

V) Prvních sedm znaků každého záznamu je uvedeno pozičně a zbývající část záznamu je uvedena ve struktuře dané znakem na pozici 7 – "P" či „O", např. 0001DP003DSLDAP199701.01.1997…. Pozičně

0001DO|003|DSL|DAP|1997|01.01.1997|…. Pomocí oddělovačů.

VI) Struktura záznamu vstupního datového souboru je daná dvěma způsoby:

a) POZIČNĚ - každá položka má stanovenou pevnou pozici OD, DO a pokud jej její délka kratší, je nutné hodnotu položky doplnit mezerami tak, aby byla dodržena pevně stanovená délka položky. Každý záznam souboru má stanovenou délku, která je rovna součtu délky všech položek záznamu.

b) POMOCÍ ODDĚLOVAČŮ – jednotlivé položky jsou od sebe odděleny stanoveným znakem (oddělovačem), a délka položek je různá. Každý záznam souboru má tedy stanovený počet oddělovačů, který je roven součtu oddělovačů mezi položkami záznamu. Stanoveným oddělovačem je zde znak ASCII sady s kódem 124 (znak „|").

VII) Každý záznam souboru je ukončen KONCEM ŘÁDKU (ASCII 13 ASCII 10).

VIII) V případě struktury POMOCÍ ODDĚLOVAČŮ musí poslední položku záznamu UKONČOVAT ODDĚLOVAČ a znak konce řádků.

I když je vstupní soubor do aplikace pro zpracování souboru v textovém formátu zde popisovaném, uložený nebo odeslaný soubor je vždy ve formátu XML.

5. VLASTNÍ NÁVRHY ŘEŠENÍ, PŘÍNOS NÁVRHU ŘEŠENÍ, EKONOMICKÉ ZHODNOCENÍ

5.1 VLASTNÍ NÁVRHY ŘEŠENÍ

Pro zabezpečení dat je nutné znát jejich cenu, dokázat ohodnotit rizika a mít ochotu investovat do protiopatření. Bezpečnost lze definovat jako zajištěnost proti hrozbám, minimalizaci rizik a komplex administrativních, technických, logických a fyzických opatření pro prevenci a detekci neautorizovaného využití dat. To jsou důvody, kde je nutné si vymezit rámec, který má na bezpečnost dat zásadní vliv.

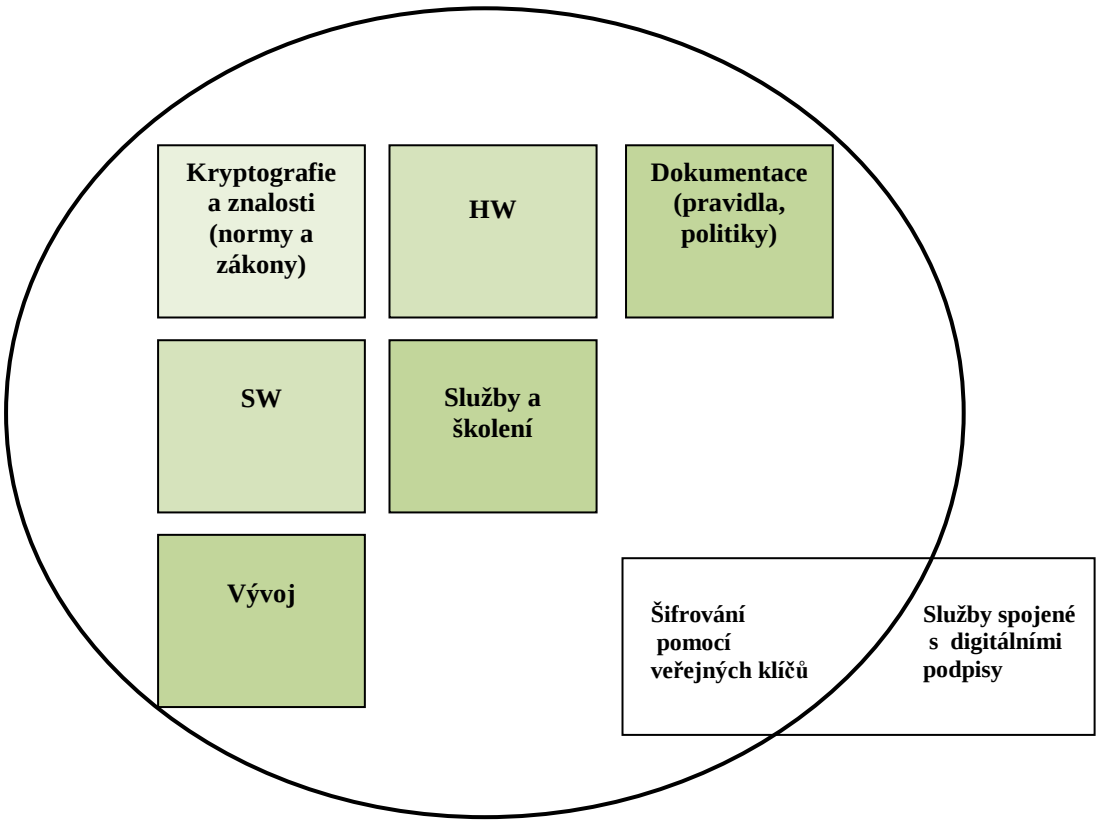
S problematikou bezpečnosti dat se nevědomky setkáváme při každodenních činnostech. V praxi nechráníme pouze soubory, ale i jiné formy dat (důležité osobní doklady, při výběru z bankomatu se snažíme zadat PIN, aniž by jej někdo mohl odpozorovat atp.). Přesto nelze vždy zabránit zneužití chráněných údajů, což bývá způsobeno tím, že hrozby a rizika se mění s technologickým pokrokem a novými postupy.

Možná opatření je třeba nastavit tak, aby veškerá rizika byla co nejvíce minimalizována.

5.1.1 PKI (Public Key Infrastructure)

Pro zajištění bezpečné komunikace a zajištění ochrany dat lze použít Integrovaný záchranný systém (dále IZS) informačního systému. Flexibilní systémy jsou dnes založeny na moderní technologii PKI, využitím asymetrické kryptografie a elektronickém podpisu. Má obrovský význam pro společné využívání informací a pro oboustranné zabezpečení informací. PKI umožňuje použít služby spojené se šifrováním a digitálními podpisy v aplikačních systémech.

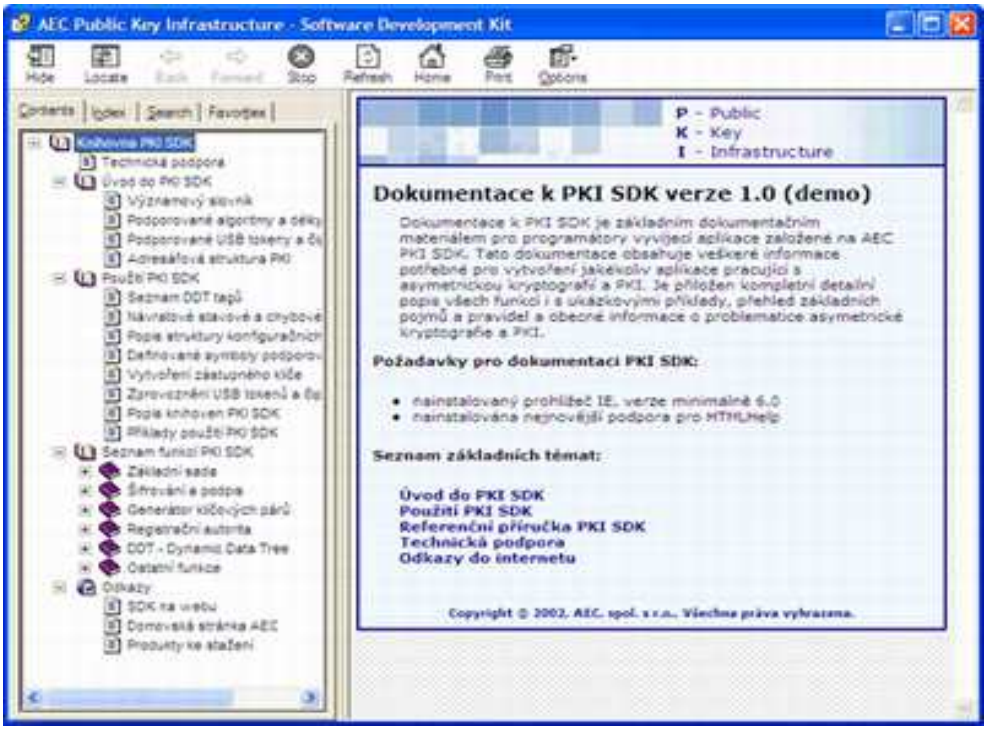
Obr. A 16: Public Key Infrastructure.[36]



Pro programátory slouží technologický nástroj *Software Development Kit (dále SDK)*, který umožňuje vývoj nových nebo úpravu existujících aplikací. V podstatě jde o několik statických a dynamických knihoven, které představují kompletní sadu modulů pro vytvoření moderních PKI aplikací.

[36] *Egovernment : PKI - základ bezpečné komunikace* [online]. 2004 [cit. 2008-05-01]. Dostupný z WWW: <http://www.egovernment.cz/prezentace%20ipe/13.ppt>

Obr. A 17: PKI SDK. [37]



Obr. A 18: Využití – implementace PKI.[38]

[37] *Egovernment : PKI - základ bezpečné komunikace* [online]. 2004 [cit. 2008-05-01]. Dostupný z WWW: <http://www.egovernment.cz/prezentace%20ipe/13.ppt>

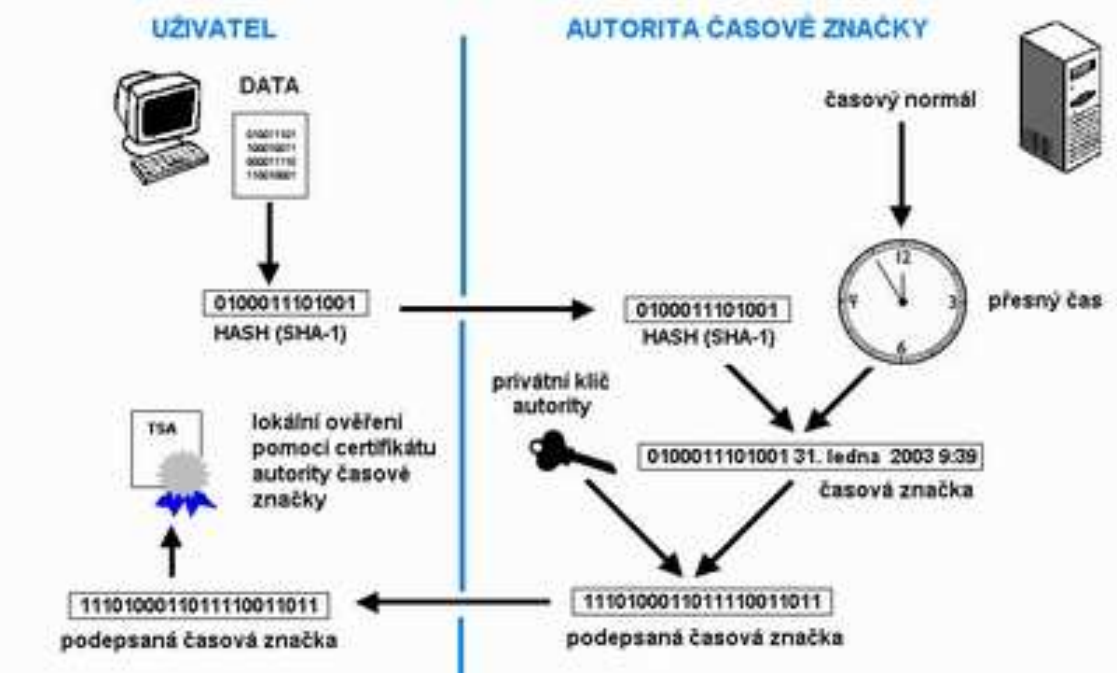
[38] *Egovernment : PKI - základ bezpečné komunikace* [online]. 2004 [cit. 2008-05-01]. Dostupný z WWW: <http://www.egovernment.cz/prezentace%20ipe/13.ppt>

5.1.2 AUTORITA ČASOVÉ ZNAČKY

Jedná se o službu, která umožňuje prokázat, že v určitém čase existoval určitý elektronický dokument, případně že byl v tomto čase elektronicky podepsán. Cílem této služby je zajistit nepopíratelnost dokumentu vzhledem k určitému času. Požadavky, které jsou s tímto cílem zasílány důvěryhodně třetí straně, přichází v určitém specifickém formátu, který je již definován příslušnými mezinárodními normami.

Autorita časových značek na žádost klienta vydává elektronické časové razítko, které má charakter elektronického certifikátu podepsaného autoritou časové značky a obsahuje mj. hash původních dat a přesný čas garantovaný autoritou. Tímto časovým razítkem lze tak opatřit jakákoli elektronická data (dokument) a zpětnou kontrolou prokázat jejich existenci před daným datem. U autority časové značky je velmi důležitý spolehlivý zdroj reálného času.

Obr. A 19: Autorita časové značky.[39]



[39] *Egovernment : PKI - základ bezpečné komunikace* [online]. 2004 [cit. 2008-05-01]. Dostupný z WWW: <http://www.egovernment.cz/prezentace%20ipe/13.ppt>.

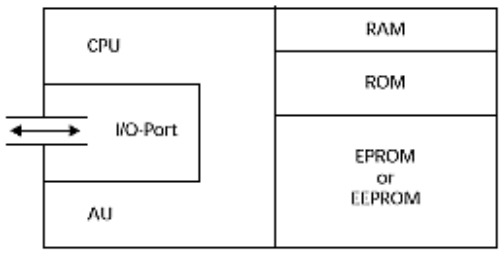
Využití časových značek

- *V mailových serverech a při komunikaci*
- *V auditech záznamech, zdravotnických záznamech*
- *V databázích*
- *V aplikacích se zvýšenými nároky na bezpečnost*
- *V elektronickém poštovním styku*
- *V archivech elektronické dokumentace*
- *V elektronickém bankovnictví*
- *V elektronických podatelnách*
- *U notářských systémů*

5.1.3 POUŽITÍ ČIPOVÝCH KARET PRO BEZPEČNOST

Kryptografické čipové karty můžeme nazvat jako počítače s vlastním operačním systémem a komunikačním rozhraním. Tyto čipové karty umožňují generování a uložení kryptografických klíčů v bezpečné paměti a provádění kryptografických operací přímo na kartě s využitím hardwarové akcelerace. Běžně jsou implementovány algoritmy DES, TDES, RSA a SHA-1, na nových čipech i AES a ECC.
Krypt. čipové karty jsou bezpečné prostředky pro mnoho aplikací (IAS, SSO…) na různých HW platformách a operačních systémech.

Obr. A 20: Čipová karta.[40]



[40] *MPSV : PKI v ISHN* [online]. [2003], 11. 7. 2007 [cit. 2008-05-01]. Dostupný z WWW: http://www.mpsv.cz/tmp/hmotna_nouze/Skoleni_informatici/Prezentace%20PKI%20a%20CK%20-%20Homolka%20-%20Brno-%20cerven%202007/PKI%20v%20ISHN.ppt.

Čipová karta a aplikace

- *OS Windows již má vestavěnou podporu čipových karet*
- *MS Outlook i Outlook Express – vestavěná podpora karet*
- *Terminál Server pro XP – podpora čipových karet pro vzdálenou práci*
- *Přihlašování do Windows s čipovou kartou (přihlášení do sítě stanice Windows 2000, XP, Active Directory)*
- *CA – certifikační autorita*
- *Single Sing-on pohodlné a bezpečné přihlašování do všech stávajících aplikací*
- *Přihlašování do WEB služeb*
- *PKI systémy: PGP, Entrust, Baltimore….*

5.1.4 STANDARDY

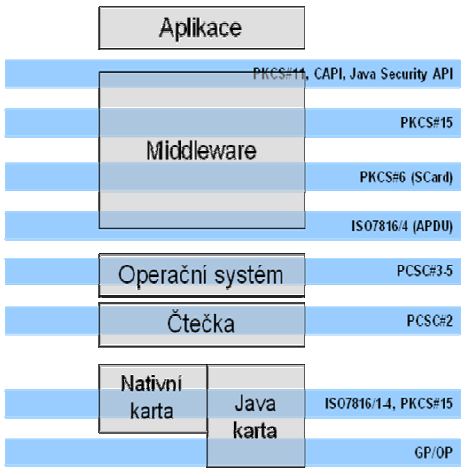
Existuje řada standardů a specifikací, které definují fyzické charakteristiky, umístění kontaktů, parametry pro kontaktní i radiovou komunikaci, metody pro zasílání příkazů a získání odpovědí, organizaci systému souborů, řízení přístupu a mnoho dalších možností.

Standard ČSN ISO/IEC 7816-15 (PKCS#15) definuje základní kryptografickou aplikaci CIA (Cryptography Information Application).

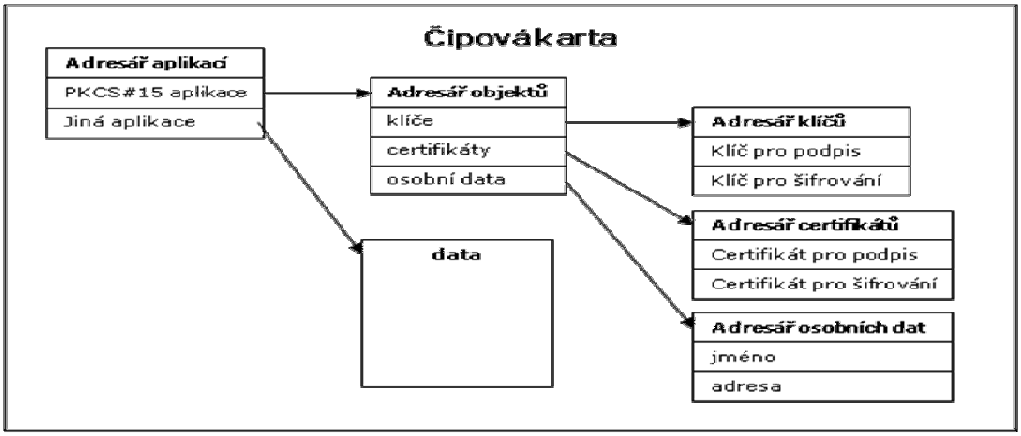
Dalším základním standardem je pak ČSN ISO/IEC 14443, uznávané specifikace tvoří Java Card a PC/SC.

I když se mezinárodní standardy nezabývají dostatečně kryptografií a krypt. rozhraním čipových karet, tak situaci zachraňují implementace PKCS#11, MS CAPI a JCE, které přispívají k interoperabilitě aplikací a kryptografických čipových karet.

Obr. A 21: Standardy.[41]



Obr. A 22: Struktura ISO/IEC 7816-15/PKCS#15.[42]



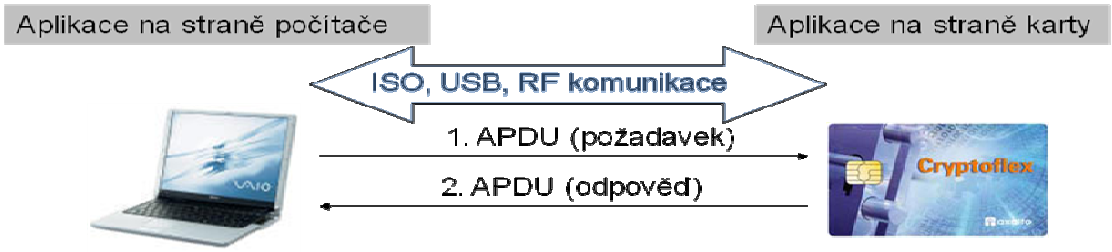
5.1.5 KOMUNIKACE

Komunikace dvou počítačů s odlišným technickým vybavením a operačním systémem. Komunikace je realizována na základě aplikačního protokolu pro mikroprocesorové čipové karty (ISO 7816-4, APDU).

[41] *ISSS : Internet ve státní správě a samosprávě* [online]. 2005 [cit. 2008-05-01]. Dostupný z WWW: <www.isss.cz/archiv/2005/download/prezentace/oksystem_rosol.ppt>.

[42] *ISSS : Internet ve státní správě a samosprávě* [online]. 2005 [cit. 2008-05-01]. Dostupný z WWW: <www.isss.cz/archiv/2005/download/prezentace/oksystem_rosol.pp.

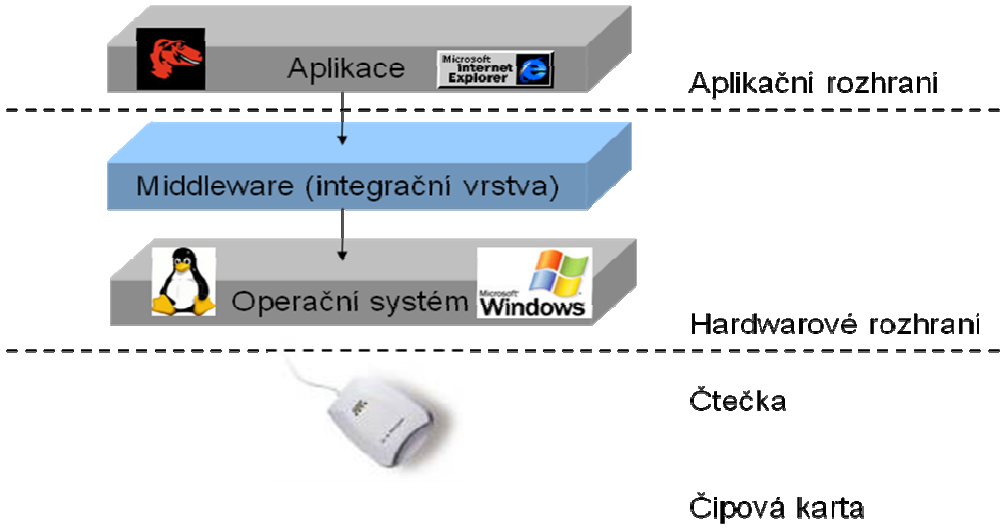
Obr. A 23: Komunikace PC s čipovou kartou.[43]



V praxi se využívají různé systémy a různé čipové karty. Postup pro zajištění jejich interoperability[44]:

- *Výběr a práce s konkrétním typem čipové karty, v rámci jediného systému (1:1).*
- *Výběr a podpora několik typů čipových karet, v rámci jediného systému (1:n).*
- *Podpora více systémů a čipových karet (m:n)*

Obr. A 24: Middleware – prostředník komunikace.[45]



Efektivní vývoj aplikací využívající čipové karty pro provádění kryptografických a datových operací musí být odstíněn od konkrétní technologie. Prostředkem k tomu jsou

[43] *MPSV : PKI v ISHN* [online]. [2003], 11. 7. 2007 [cit. 2008-05-01]. Dostupný z WWW: http://www.mpsv.cz/tmp/hmotna_nouze/Skoleni_informatici/Prezentace%20PKI%20a%20CK%20-%20Homolka%20-%20Brno-%20cerven%202007/PKI%20v%20ISHN.ppt.

[44] Interoperabilita – schopnost vzájemně si rozumět, vzájemně spolupracovat.

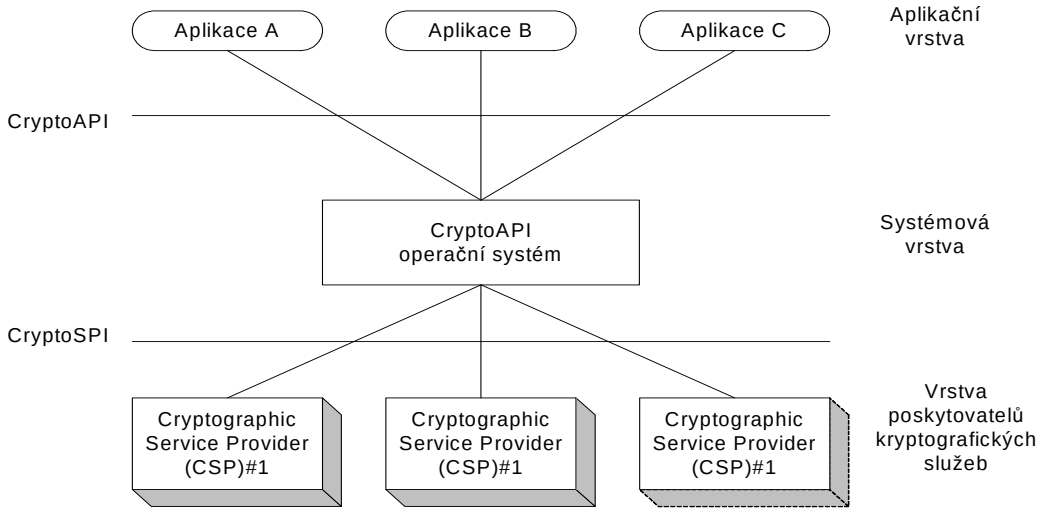
[45] *ISSS : Internet ve státní správě a samosprávě* [online]. 2005 [cit. 2008-05-01]. Dostupný z WWW: <www.isss.cz/archiv/2005/download/prezentace/oksystem_rosol.ppt>.

kryptografická rozhraní definovaná v rámci jednotlivých platforem nebo operačních systémů.

WINDOWS – CryptoAPI a CSP

Microsoft **Crypto API** (MS CAPI) je proprietární[46] architektura firmy MS použitá v systémech Windows. Aplikace mohou využívat alternativní kryptografické služby prostřednictví standardního rozhraní bez nutnosti komunikovat přímo s konkrétním CSP. Aplikace jsou realizovány pomocí dynamických knihoven Advapi32.dll a Crypto32.dll operačního systému Windows.

Obr. A 25: Crypto API a CSP.[47]



CSP udržuje privátní/ veřejné klíče v permanentní paměti v tzv. kontejnerech, umístěných v technickém zařízení nebo v zašifrovaném tvaru na disku. MS definuje funkce CSP (syntaxi, vstupní, výstupní a návratové hodnoty) a umožňuje dodat vlastní

[46] Proprietární – komerční.

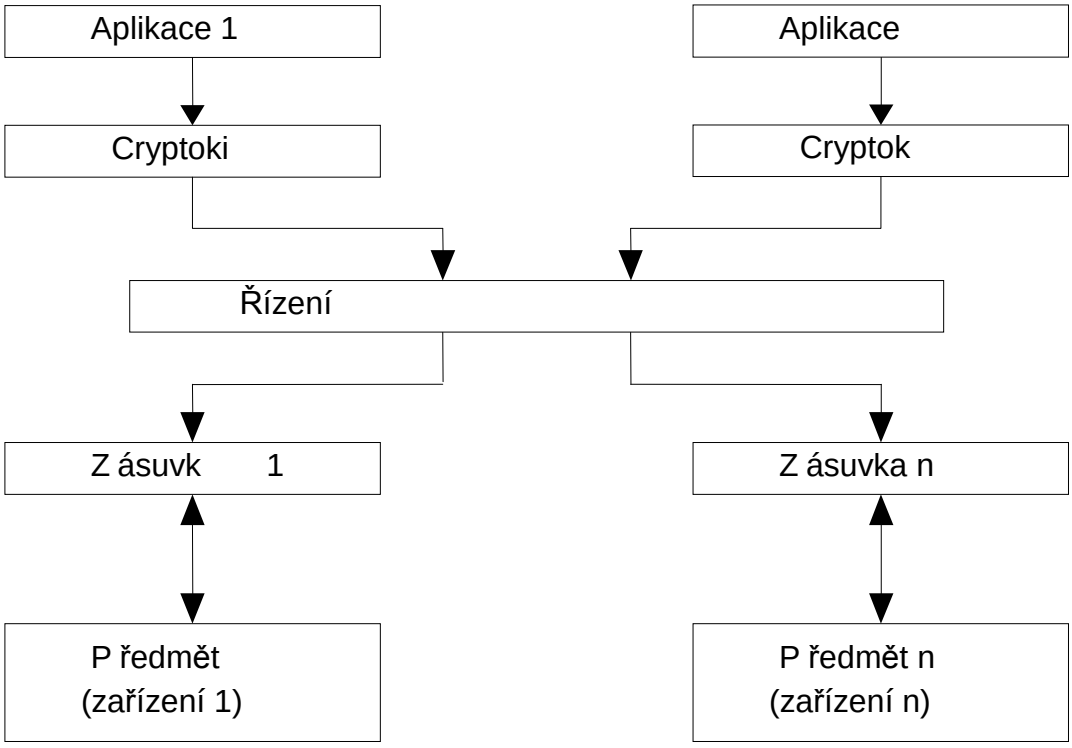
[47] *ISSS : Internet ve státní správě a samosprávě* [online]. 2005 [cit. 2008-05-01]. Dostupný z WWW: <www.isss.cz/archiv/2005/download/prezentace/oksystem_rosol.ppt>.

CSP, kde jsou podporovány různé kryptoalgoritmy. Vlastní CSP musí: exportovat stanovené funkce CryptoSPI, elektronicky podepsán firmou Microsoft.

API nezávislé na systému -PKCS#11

Toto rozhraní je navrženo bez závislosti na použitém operačním systému a je nejpoužívanějším kryptografickým rozhraním mimo platformu Windows. Je primárně svázáno s programovacím jazykem C/C++. Z běžných aplikací toto rozhraní používá internetový prohlížeč Mozilla a jeho poštovní klient, Lotus Notes, Entrust atd.

Obr. A 26: Model PKCS#11.[48]

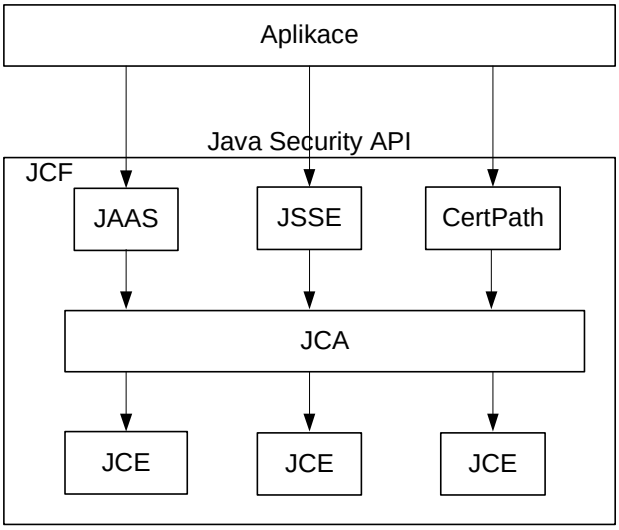


Platforma Java – JCA/JCE

[48] *ISSS : Internet ve státní správě a samosprávě* [online]. 2005 [cit. 2008-05-01]. Dostupný z WWW: <www.isss.cz/archiv/2005/download/prezentace/oksystem_rosol.ppt>.

Java aplikace může využít několik pokročilých API – Java Authentication and Authorisation Service (JAAS), Java Secure Socket Extension (JSSE), Java Certification Path a Java Generic Security Services (GSS-API).
Kryptografické funkce jsou implementovány v rámci připojitelných modulů Java Cryptography Extension (JCE).

Obr. A 27: Platforma Java – JCA/JCE.[49]

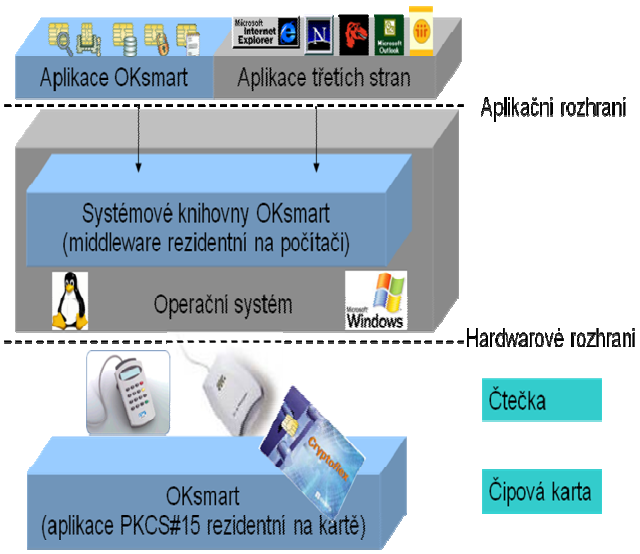


5.1.6 MIDDLEWARE OKsmart

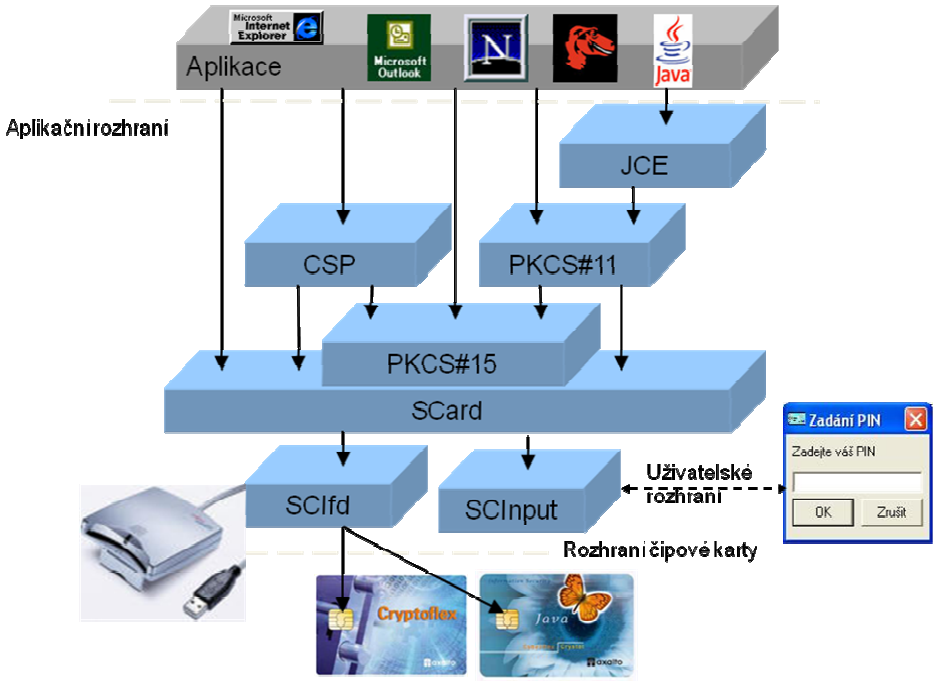
Ok smart je softwarové řešení pro transparentní integraci kryptografických čipových karet do prostředí Windows a Linux s maximálním respektováním standardů.

[49] *ISSS : Internet ve státní správě a samosprávě* [online]. 2005 [cit. 2008-05-01]. Dostupný z WWW: <www.isss.cz/archiv/2005/download/prezentace/oksystem_rosol.ppt>.

Obr. A 28: Komponenty OKsmart.[50]



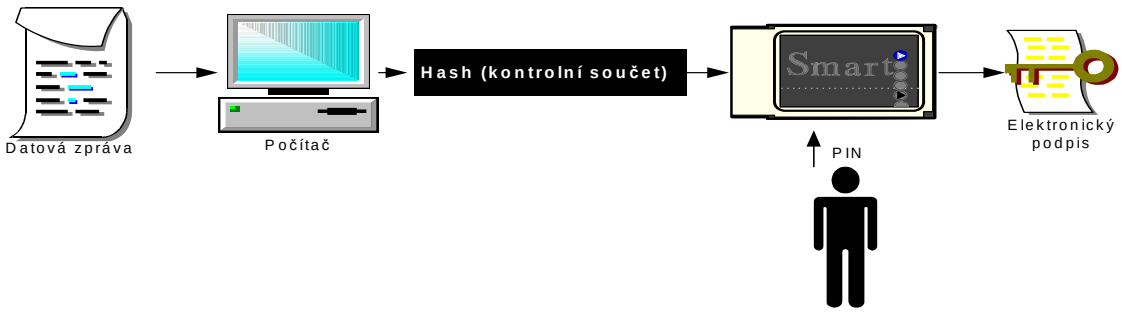
Obr. A 29: Architektura OKsmart.[51]



[50] *MPSV : PKI v ISHN* [online]. [2003], 11. 7. 2007 [cit. 2008-05-01]. Dostupný z WWW: <http://www.mpsv.cz/tmp/hmotna_nouze/Skoleni_informatici/Prezentace%20PKI%20a%20CK%20-%20Homolka%20-%20Brno-%20cerven%202007/PKI%20v%20ISHN.ppt>.

[51] *ISSS : Internet ve státní správě a samosprávě* [online]. 2005 [cit. 2008-05-01]. Dostupný z WWW: <www.isss.cz/archiv/2005/download/prezentace/oksystem_rosol.ppt>.

Obr. A 30: Elektronický podpis s čipovou kartou.[52]



5.2 PŘÍNOS NÁVRHU ŘEŠENÍ

Klíčovým úkolem je bezpečná identifikace a autentizace, ochrana při nepřítomnosti, realizace bezpečných plateb a zajištění ochrany elektronického podpisu proti zneužití.
Pomocí základních bezpečnostních nástrojů lze těmto hrozbám do jisté míry zabránit. (PIN, biometrika, šifrování atd.).

Efektivním nástrojem pro „silnější“ autentizaci uživatelů je PKI (Public Key Infrastructure). Zde každý uživatel a služba vlastní certifikát veřejného klíče podepsaný některou důvěryhodnou certifikační autoritou (CA).
Každý uživatel má certifikát, kde odpovídající soukromý klíč je heslem zašifrovaný a uložen na disku. Aby se předcházelo zadávání hesla při každém přístupu k požadovaným informačním zdrojům, nabízí PKI tzv. proxy certifikáty. Jedná se o nově vygenerovaný certifikát, který není podepsán žádnou CA, ale uživatelovým vlastním soukromým klíčem. Má platnost několik málo hodin a je čitelný pouze pro majitele certifikátu. Krátká doba platnosti proxy certifikátu snižuje riziko zneužití proti případnému ukradení certifikátu.
Pro autorizaci se používají tzv. atributové certifikáty. Mají podobnou strukturu jako certifikáty veřejných klíčů. Tyto certifikáty neobsahují veřejné klíče, ale sadu atributů

[52] *MPSV : PKI v ISHN* [online]. [2003], 11. 7. 2007 [cit. 2008-05-01]. Dostupný z WWW: <http://www.mpsv.cz/tmp/hmotna_nouze/Skoleni_informatici/Prezentace%20PKI%20a%20CK%20-%20Homolka%20-%20Brno-%20cerven%202007/PKI%20v%20ISHN.ppt>.

spojených s držitelem, jako je např. příslušnost do skupiny, role, oprávnění a další údaje, na základě kterých jsou uživateli přidělena přístupová práva. Platnost je i zde časově omezena. Atributový certifikát je podepsán službou, která ho vydala a koncový server jen ověří podpis na certifikátu a zkontroluje příslušné atributy. Atributový certifikát je součástí autentizačního procesu a je zakódován v uživatelově proxy certifikátu.
Takové prostředí umožňuje přiřadit uživateli taková přístupová oprávnění, jež potřebuje pro svou práci.
Použití PKI je výborným nástrojem k prokazování identity a to tam, kde je požadována silná autentizace. Při autentizaci není nutné, aby byl uživatel zaveden v adresáři. PKI je podporována v operačních systémech a ve webových aplikacích.

Pro kvalitní a vysoké zabezpečení jsou nejvíce vhodné kryptografické čipové karty. Jedná se o pokročilý kryptografický prostředek, který je klíčem k bezpečné komunikaci a přístupu k informacím. Tento prostředek nám umožňuje vytvářet aplikace nezávislé.

Výhody čipové karty

- Mobilita
- Kompaktnost a rozměry
- Vysoké zabezpečení pro elektronický podpis
- Privátní klíč nikdy neopouští kartu
- Bezpečné úložiště dat
- Spolehlivé úložiště dat
- Nezkopírovatelnost karty
- Prestižní image

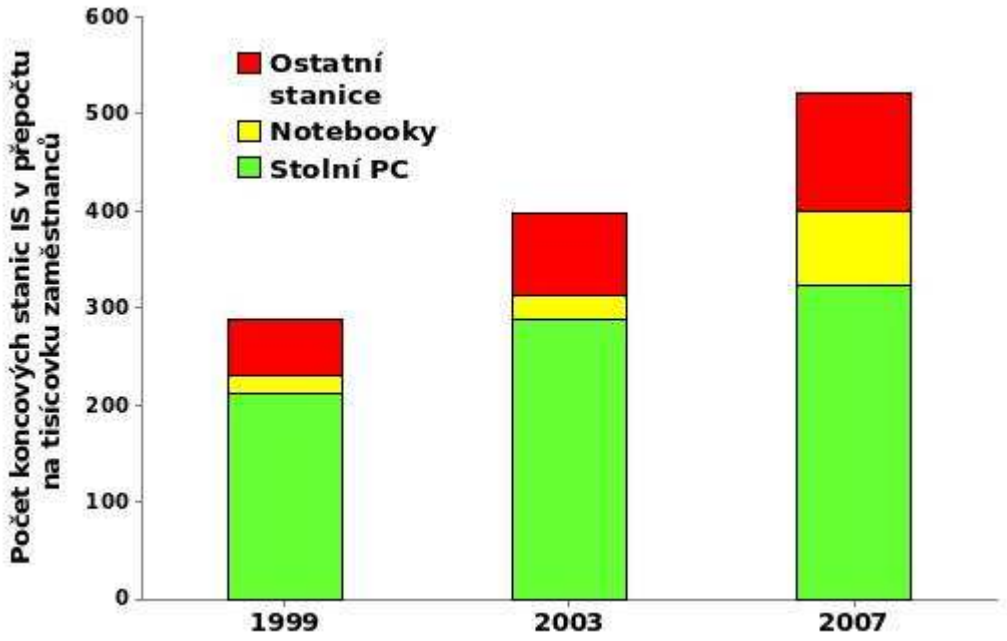
Nevýhody

- Nesnadná dostupnost karet i čteček
- Nedostatek informací
- Nedostatek zkušeností s jejich využitím
- Nízká kapacita pro vlastní data

5.3 EKONOMICKÉ ZHODNOCENÍ

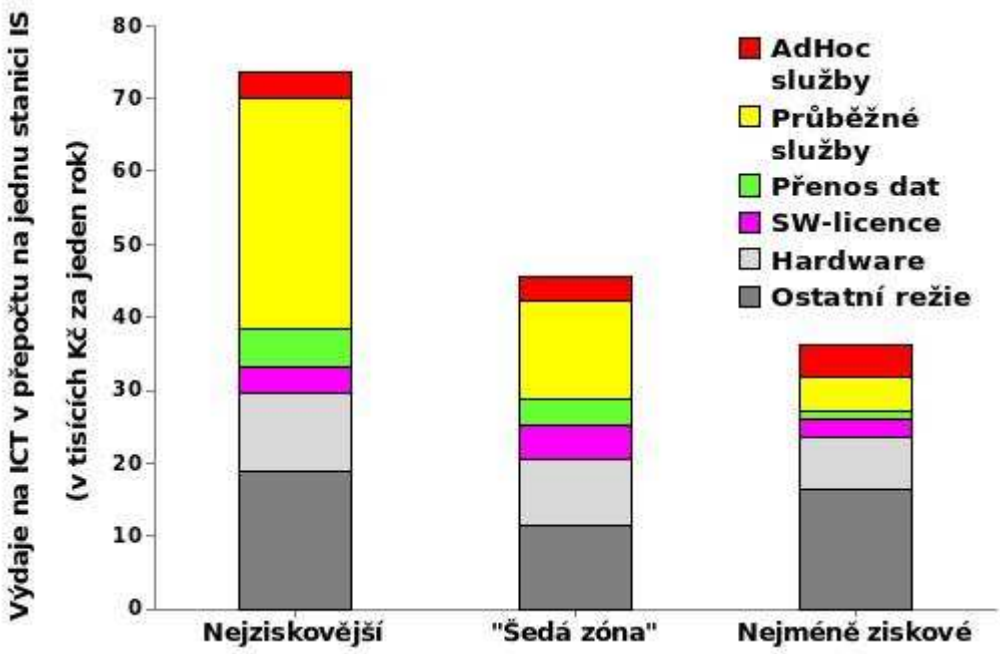
Základem podnikových informačních systémů českých podniků se již v minulém desetiletí staly stolní osobní počítače. Těmi tak byli již na konci devadesátých let minulého století vybaveni prakticky všichni manažeři, obchodníci a ostatní administrativní i techničtí pracovníci českých podniků. S růstem počtu koncových stanic informačních systémů se však také začala stále výrazněji měnit jejich struktura. Ještě rychleji, než stolní osobní počítače začaly přibývat spolu s notebooky také další typy koncových stanic informačních systémů, jako jsou mobilní příruční počítače s integrovanými snímači čárových kódů či specializované pokladní terminály.

Obr. A 31: Počet koncových stanic informačních systémů ve firmách.[53]



[53] KARPECKI, Lubomír. *Spis: Informační technologie v českých podnicích* [online]. [2003] [cit. 2008-05-01]. Dostupný z WWW: <http://www.spis.cz/spis2/index.php?id=1250>.

Obr. A 32 Výdaje na informační a komunikační technologie.[54]



Vyčíslení efektů z úspory času pracovníka při zpracování dokladu v cyklu objednávka – faktura

Předpoklady:

- mzdové náklady pracovníka 100 Kč/ hod.
- nominální časový fond pracovníka 200 dní / rok

Časová úspora 15 minut / doklad

Tab. 5: Úspora nákladů při zavedení elektronického dokladu.[55]

Počet dokumentů denně	Úspora času (hod.)	Úspora peněz (Kč)
10	500	50000
50	2500	250000
100	5000	500000
200	10000	1000000

[54] KARPECKI, Lubomír. *Spis: Informační technologie v českých podnicích* [online]. [2003] [cit. 2008-05-01]. Dostupný z WWW: <http://www.spis.cz/spis2/index.php?id=1250>.

[55] Papírový versus elektronický dokument. *ISVS* [online]. 2007 [cit. 2008-05-01]. Dostupný z WWW: http://www.isvs.cz/e-podpis-podatelny/papirovy-versus-elektronicky-dokument-27-dil.html.

Vyčíslení efektů z úspory peněžních prostředků na tisk, poštovné a související výdaje:

- 10 Kč na straně odesilatele (upraveno dle dokumentu Sdružení pro informační společnost – Normální je fakturovat elektronicky).
- 30 Kč na straně příjemce.
- Kalkulace rovněž na 200 dní / rok.

Tab. 6: Vyčíslení efektů z úspory peněžních prostředků.[56]

Počet dokumentů denně	Náklady odesílatele (Kč)	Náklady příjemce (Kč)	Celkem ročně (Kč)
10	100	300	80000
50	500	1500	400000
100	1000	3000	800000
200	2000	6000	1600000

Pro komunikaci s orgány veřejné správy s využitím elektronického podpisu si musí občan pořídit tzv. kvalifikovaný certifikát. V současné době jsou v ČR akreditovány tři subjekty, které jsou oprávněny tyto kvalifikované certifikáty vydávat:

I) První certifikační autorita, a. s.
II) Česká pošta, s. p.
III) eIdentity, a. s.

Tab. 7: Cena kvalifikovaných certifikátů dle jednotlivých poskytovatelů.[57]

První certifikační autorita, a. s.	**632 Kč (Standard)**
	1452 Kč (Comfort)
Česká pošta, s. p.	**160 Kč**
eIdentity, a. s.	**590 Kč**

[56] Papírový versus elektronický dokument. *ISVS* [online]. 2007 [cit. 2008-05-01]. Dostupný z WWW: <http://www.isvs.cz/e-podpis-podatelny/papirovy-versus-elektronicky-dokument-27-dil.html>

[57] *CZECHINVEST: e-podpis* [online]. 1994-2008 [cit. 2008-05-01]. Dostupný z WWW: <www.czechinvest.org/data/files/e-podpis-185.pdf>.

6. ZÁVĚR

S rozvojem internetu jako zdroj obrovského množství informací se vyvíjí také nová „digitální“ ekonomika. To vedlo samozřejmě k vytvoření mnoha různých elektronických platebních nástrojů a metod v elektronickém obchodování.

I přesto, že klasické platební systémy mají stále navrch oproti těm elektronickým, je ale zřejmé, že elektronické platební modely přináší člověku jednoduchost, šetří mu čas a finanční prostředky a mají další výhody. Tento druh e-komunikace také sebou přináší počítačovou kriminalitu, která se pomocí nových technologií vyvíjí stejně rychle jako samotný fenomén „Internet“.

Mezi nejvýznamnější zápor je nedůvěra uživatelů v dostatečnou ochranu osobních dat. Zařízení postavená na kryptografických čipových kartách v současné době poskytují dostatečnou míru bezpečnosti pro mnoho aplikací. Tyto zařízení se týkají především elektronického bankovnictví a elektronických daňových přiznání.

Na první pohled se zdá, že celá oblast možnosti podávat a podepisovat elektronické dokumenty v kontaktu se státní správou poněkud nepřehledná. Proto také v současné době převyšuje počet fyzického podání (zdlouhavého papírování) oproti elektronickému podání (EPO), které je podstatně snadnější, rychlejší, méně nákladnějším. Česká republika se vyznačuje jistým konzervatismem, kdy lidé mají větší důvěru v osobní podání než k elektronickému podání. Postupem času však EPO (elektronické podání) používá čím dál více uživatelů a stává se tak významnou součástí komunikace s Českou daňovou správou.

Velmi účinné se jeví propojení firewallu a proxy serveru pro přístup internetu nebo antivirového systému pro firewally. Síť je pak chráněna nejen proti útoku, ale i proti počítačovým virům a červům, které jsou odchyceny antivirovým systémem.

Budoucnost bezpečné elektronické komunikace vidím právě v kryptografických čipových kartách s elektronickým podpisem. Velkým kladem je jejich multifunkčnost, lze je tedy využít na více věcí, než pouze placení. Budou-li plně využity technologické možnosti čipových karet, byla by schopna obsahovat kromě platební funkce i průkaz zdravotní pojišťovny, elektronický řidičský průkaz atd.

V návaznosti na čipové kartě je nutné zmínit se také o novém trendu vývoje v oblasti bezpečnosti zvaném biometrika. Jedná se o ověření totožnosti pomocí různých částí těla (otisk prstu, sítnice oka atd.). Tento trend bude v budoucnu hrát jednoznačně velkou roli.

Vypracováním této práce jsem poznal detailněji význam a princip elektronického podepisování, elektronických dokumentů a bezpečnosti elektronické komunikace.
Mým cílem bylo poskytnutí základních informací o bezpečnosti dat a o elektronickém podpisu v e-dokumentech. Domnívám se, že jsem tento cíl splnil.

7. POUŽITÉ INFORMAČNÍ ZDROJE

(1) KRAS, P. *Internet v kostce*. 2. Vydání, Havličkův Brod: Fragment, 2002. 144 s. ISBN 80-7200-510-3.

(2) DOSEDEL, T. *Počítačová bezpečnost a ochrana dat*. 1. Vydání, Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

(3)SLAISOVÁ, Jarmila: Prakticky nepraktický elektronický podpis. *Ikaros* [online]. 2001, č. 6 [cit. 2001-06-04]. ISSN 1212-5075. Dostupný z WWW: http://ikaros.ff.cuni.cz/2001/c06/podpis.htm.

(4)Papírový versus elektronický dokument. *ISVS* [online]. 2007 [cit. 2008-05-01]. Dostupný z WWW: http://www.isvs.cz/e-podpis-podatelny/papirovy-versus-elektronicky-dokument-27-dil.html.

(5)HRUBÝ, Jaroslav; MOKOŠ, Igor: Elektronický podpis: Je to bezpečné? *Computer World* [online]. 2001, č. 27. ISSN 1210-9924. C01C1178.TXT. [cit. 2001-11-24]. Dostupný z WWW:http://www.cw.cz/cwarchiv.nsf/byID/E6CADA9664281571C1256AB1005617C7?OpenDocument.

(6)ROČNÍ ZPRÁVA 2006: O ministerstvu financí, organizační složce státu, v kapitole 312 státního rozpočtu. *MFČR* [online]. 2006 [cit. 2008-03-03], s. 1-28. Dostupný z WWW: http://www.mfcr.cz.

(7)Finance.cz: Poznejte hodnotu informace [online]. c2000 [cit. 2008-02-20]. Dostupný z WWW: <http://www.finance.cz/. ISSN 1213-432.

(8)Ministerstvo financí ČR [online]. c2005 [cit. 2008-02-20]. Dostupný z WWW: <http://www.mfcr.cz/cps/rde/xchg/.

(9)COMPUTERWORLD: Deník pro IT profesionály [online]. c2006 [cit. 2008-02-20]. Dostupný z WWW: <http://www.computerworld.cz/.

(10)Statnisprava.cz [online]. c2000 [cit. 2008-02-20]. Dostupný z WWW: <http://www.statnisprava.cz/.

(11)E-komerce.cz: Váš bussines na internetu [online]. c1998 [cit. 2008-02-20]. Dostupný z WWW: <http://www.e-komerce.cz/.

(12)BussinesInfo.cz: Oficiální portál pro podnikání a export [online]. c1997 [cit. 2008-02-20]. Dostupný z WWW: <http://www.businessinfo.cz/cz/.

(13)WIKIPEDIE: Otevřená encyklopedie [online]. 2002 [cit. 2008-02-20]. Dostupný z WWW: <http://cs.wikipedia.org/.

(14)ISVS.CZ: Informační Systémy Veřejné Správy [online]. c2001 [cit. 2008-02-20]. Dostupný z WWW: <http://www.isvs.cz/>. ISSN 1802-6575.

(15)Úřad *pro ochranu osobních údajů: the office for personal data protection* [online]. c200 , 18. 12. 2007 [cit. 2008-02-20]. Dostupný z WWW: <http://www.uoou.cz/.

(16)AxonNet [online]. c2006 [cit. 2008-02-20]. Dostupný z WWW: <http://www.axonnet.cz/.

(17)Www.dbsvet.cz [online]. c2004 [cit. 2008-02-20]. Dostupný z WWW: <http://www.dbsvet.cz/. ISSN 1213-5933.

(18)PC-politika.com [online]. c2004 , 8. 8. 2007 [cit. 2008-02-20]. Dostupný z WWW: <http://www.pc-politika.com/.

(19)*KHnetWiki* [online]. [2006], 27. 10. 2007 [cit. 2008-02-20]. Dostupný z WWW: <http://wiki.khnet.info/.

(20) *STÁTNÍ TÍSKÁRNA CENIN* [online]. [2005] [cit. 2008-03-05]. Dostupný z WWW: <http://www.stc.cz/.

(21)Úřad pro zastupování státu ve věcech majetkových [online]. c2002-2008 , 10. 3. 2008 [cit. 2008-03-10]. Dostupný z WWW: <http://www.uzsvm.cz/.

(22)Archiv stránek bývalého Ministerstva informatiky: Elektronické komunikace [online]. [2000] [cit. 2008-05-01]. Dostupný z WWW: http://www.mvcr.cz/micr/ekomunikace/default.htm.

(23)MF: Elektronické zpracování písemnosti [online]. 1999-2006 [cit. 2008-05-01]. Dostupný z WWW: http://adisepo.mfcr.cz/adis/jepo/.

(24)VOJTĚCH, Kačmařík. *Výuková podpora předmětu internetové technologie* [online]. [2006] [cit. 2008-05-01]. Dostupný z WWW: <http://homel.vsb.cz/~kac061>.

(25)Česká daňová správa [online]. 2006 [cit. 2008-05-01]. Dostupný z WWW: <http://cds.mfcr.cz>.

R E J S T Ř Í K

8. PŘÍLOHY

SEZNAM OBRÁZKŮ

Příloha A: INFORMAČNÍ ZDROJE

HRUBÝ, Jaroslav; MOKOŠ, Igor: Elektronický podpis: Je to bezpečné? *Computer World* [online]. 2001, č. 27. ISSN 1210-9924. C01C1178.TXT. [cit. 2001-11-24]. Dostupnýz WWW:http://www.cw.cz/cwarchiv.nsf/byID/E6CADA9664281571C1256AB1005617C7?OpenDocument.

PETERKA, Jiří: Kdy bude elektronický podpis na úřadech? *In: eArchiv. Články, přednášky a tutoriály J. Peterky* [online]. 2001. [cit. 2001-09-03]. Dostupný z WWW: http://archiv.czech.net/b01/b0900001.php3.

SLOVENSKÁ INFORMATICKÁ SPOLOČNOST. ODBORNÁ SKUPINA SLOVENSKEJ INFORMATICKEJ SPOLOČNOSTI: *Odborná skupina Slovenskej informatickej spolocnosti pre pripravu Zákona o elektronickom podpise* [online]. 2000. [cit. 2000-11-19]. Dostupný z WWW: http://www.informatika.sk/lat/e-podpis.

STOLZ, John S.; CROMIE, John D.: *Elecronic Signatures in Global and National Commerce Act* [online]. New Jersey: Connell Foley LLP, 2001. Articles. Dostupný z WWW: http://www.cfg-lawfirm.com/articles/oneclick.html.

LOPOUR, D. EDI komunikace v ČR. *Moderní obchod*: časopis *pro úspěch v prodeji*. 1. 1. 2007, roč. 15, č. 11, s. 32-34. ISSN 1210-4094.

SODOMKA, P. IT v dodavatelských řetězcích: Komunikace s podporou EDI a RFID. *Connect!*. 1. 1. 2006, roč. 11, č. 11, s. 18-19. ISSN 1211-3085.

MCCULLAGH, Adrian; LITTLE, Peter; CAELLI William: Electronic Signatures : Understand the Past to Develop the Future. *The University of New South Wales Law Journal* [online]. 1998, vol. 2, no. 2. ISSN 0313-0096. [cit. 1998-10-30]. Dostupný z WWW: http://www.austlii.edu.au/au/other/unswlj/thematic/1998/vol21no2/mccullagh.html.

ŠLAISOVÁ, Jarmila: Prakticky nepraktický elektronický podpis. *Ikaros* [online]. 2001, č. 6 [cit. 2001-06-04]. ISSN 1212-5075. Dostupný z WWW: http://ikaros.ff.cuni.cz/2001/c06/podpis.htm.

MATĚJKA, Jan: *Elektronický podpis v právu ES* [online]. 2001. [cit. 2001-03-28]. Dostupný z WWW: http://eu.juristic.cz/70586.

Orange *Group, a.s.: Rizika úniku informací* [online]. 2008 [cit. 2008-04-30]. Dostupný z WWW: <http://vycvik.orangegroup.cz/index.php?cnt=dtl&id=6>.

POUR, J. *Informační systémy a elektronické podnikání*. 1. Vydání, Praha: Vysoká škola ekonomická, Fakulta informatiky a statistiky, 2001. 221 s. ISBN 80-245-0227-5

DOSTÁLEK, L; VOHNOUTOVÁ, M.. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 1. Vydání, Brno: Computer Press, 2006. 534 s. ISBN 80-251-0828-7.

ŠVADLENKA, L.; MADLEŇÁK, R. Elektronické obchodování. 1. Vydání, Pardubice: Institut Jana Pernera, 2007. 163 s. ISBN 978-80-86530-40-6.

PORADA, V; RAK, R. *Kriminalita související s informačními a komunikačními technologiemi a identifikace osob na základě projevu lokomoce člověka: (vybrané problémové okruhy výzkumu)*. 1. Vydání, Praha; Karlovy Vary: Vysoká škola Karlovy Vary, 2007. 261 s. ISBN 978-80-254-0797-4.

MLÝNEK, J. *Zabezpečení obchodních informací*. 1. Vydání, Brno: Computer Press, c2007. 154 s. ISBN 978-80-251-1511-4.

ČANDÍK, M. *Bezpečnosť informačných systémov, steganografia a digitálna vodotlač*. Ostrava: s. n., c2005. 117 s. ISBN 80-239-5962-X .

JAŠEK, R. *Informační a datová bezepčnost*.1. Vydání, Zlín: Univerzita Tomáše Bati ve Zlíně, 2006.140 s. ISBN 80-7318-456-7.

M. Kuba, Web Services, Zpravodaj ÚVT MU, ISSN 1212-0901, 2003, roč. 13, č.3, s.9-14. Dostupný z WWW: http://www.ics.muni.cz/bulletin/issues/vol13num03/kuba2/kuba2.html.

Miroslav Žák, XML - začínáme programovat, Grada Publishing s.r.o., Praha 2003, ISBN 80-247-0565-6.

Gerald Carter, O'Reilly, LDAP System Administration, March 2003, ISBN 1-56592-491-6M.

D. Kouřil, Certifikáty veřejných klíčů, Zpravodaj ÚVT MU, ISSN 1212-0901, 2000, roč.10, č.4, s.5-9. Dostupný z WWW: http://www.ics.muni.cz/bulletin/issues/vol10num04/kouril/kouril.html.

W3C : Digital Signature Label Architecture [online]. 1997 [cit. 2008-05-01]. Dostupný z WWW: <http://www.w3.org/TR/WD-DSIG-label-arch.html>.

Cryptography World : Cryptography Made Easier [online]. 2004-2005 [cit. 2008-05-01]. Dostupný z WWW: <http://www.cryptographyworld.com/>.

Sun : microsystems [online]. 1994-2008 [cit. 2008-05-01]. Dostupný z WWW: <http://www.sun.com/>.

Open SSL Documents [online]. [2003] [cit. 2008-05-01]. Dostupný z WWW: <http://www.openssl.org/docs/>.

Příloha B: ELEKTRONICKÉ PODÁNÍ

Obr. B 1: Počet elektronických podání prostřednictvím EPO

ROK	2004	2005	2006	2007 (K 31.7.)
Počet podání	15 391	40 469	91 408	90 006

Zdroj: *Česká daňová správa* [online]. 2006 [cit. 2008-05-01]. Dostupný z WWW: <http://cds.mfcr.cz>.

Aktuální verze (EPO) umožňuje zpracování následujících písemností:

Daňová informační schránka

DPRZA1 – Žádost o zřízení daňové informační schránky

DPRZA2 – Žádost o rušení daňové informační schránky

DPRZA3 – Přihláška k nahlížení do daňové informační schránky

DPRPM1 – Plná moc neomezená

DPRPM2 – Plná moc

Daň z přidané hodnoty

DPHDP1 – Přiznání k dani z přidané hodnoty platné od 1. 5. 2004

DPHDAP – Přiznání k dani z přidané hodnoty platné do 30. 4. 2004

DPHSHV – Souhrnné hlášení VIES

Daň z příjmů fyzických osob

DPFDP2 – Daň z příjmů fyzických osob – pouze pro zdaň.období roku 2007

DPFDP1 – Daň z příjmů fyzických osob – pouze pro zdaň.období roku 2006

DPFDAP – Daň z příjmů fyzických osob – pouze pro zdaň.období roku 2005

DPFDB1 – Daň z příjmů fyzických osob – typ B – pro rok 2004

DPFDPB – Daň z příjmů fyzických osob – typ B – pro rok 2003

DPFDPA – Daň z příjmů fyzických osob – typ A – 2003 -2004

Daň z příjmů právnických osob

DPPDP4 – Daň z příjmů právnických osob – zdaň.období započatá v r. 2007
DPPDP3 – Daň z příjmů právnických osob – zdaň.období započatá v r. 2006
DPPDP2 – Daň z příjmů právnických osob – zdaň.období započatá v r. 2005
DPPDP1 – Daň z příjmů právnických osob – zdaň.období započatá v r. 2004
DPPDAP – Daň z příjmů právnických osob – zdaň.období započatá v r. 2003

Závislá činnost
DPZVD3 – Vyúčtování daně z příjmů FO ze závislé činnosti a z funkčních požitků včetně všech příloh – pouze pro zdaňovací období roku 2007.
DPZVD2 – Vyúčtování daně z příjmů fyzických osob ze závislé činnosti a z funkčních prožitků včetně všech příloh – pouze pro zdaňovací období roku 2006.
DPZVDA – Vyúčtování daně z příjmů fyzických osob ze závislé činnosti a z funkčních prožitků včetně všech příloh – pouze pro zdaňovací období roku 2005.

Daň silniční
DSLDAP – Daňové přiznání k dani silniční

Daň z nemovitostí
DNEDP2 – Daňové přiznání k dani z nemovitostí – od roku 2007.
DNEDAP – Daňové přiznání k dani z nemovitostí – pouze do roku 2006.

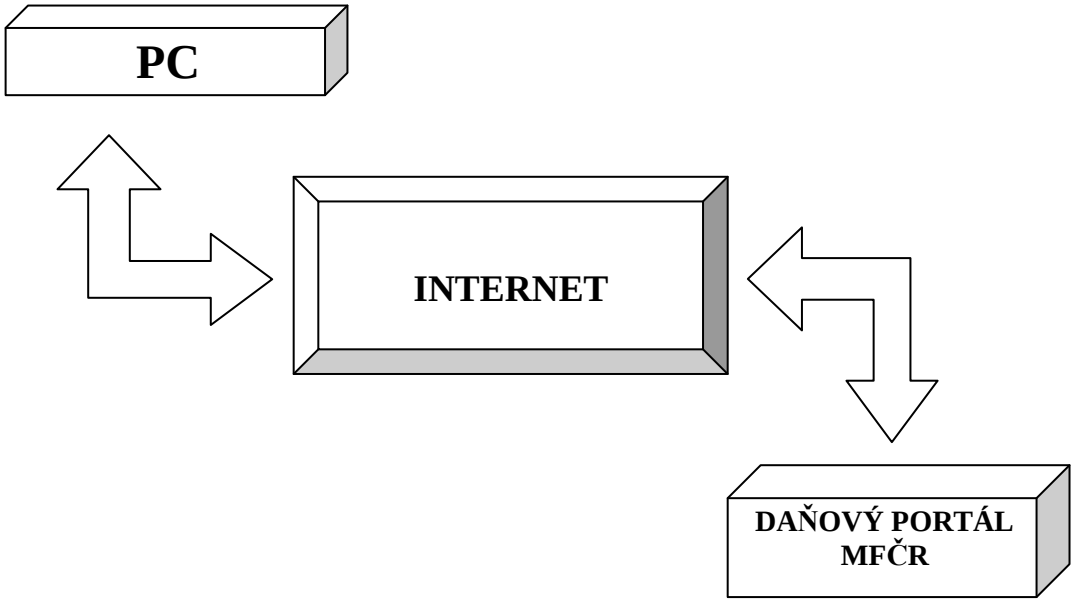
Oznámení podle § 34 zákona č.337/1992 Sb.
RHLOZN – Oznámení o nezdaněných vyplacených částkách fyzickým osobám.

Hlášení platebního zprostředkovatele
MPDHPZ – Hlášení platebního zprostředkovatele podle §38fa zákona 581/1992 Sb.

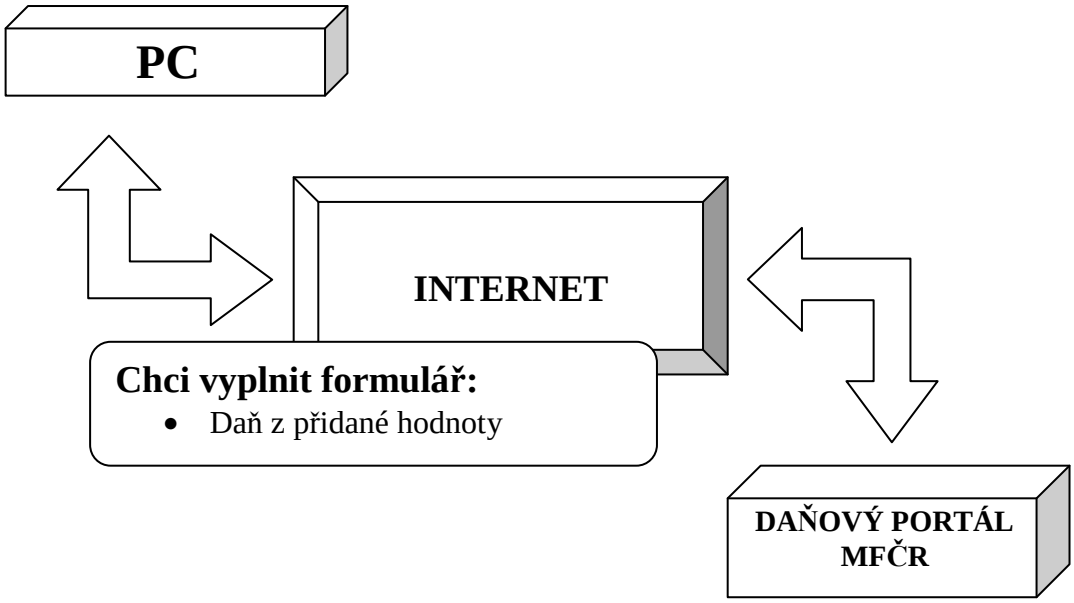
Obecné písemnosti
DADPIS – Obecná písemnost určena pro finanční úřad, finanční ředitelství nebo MF
DADSOB – Obecná písemnost určení pro podání státních orgánů a bank

Postup elektronického podání:

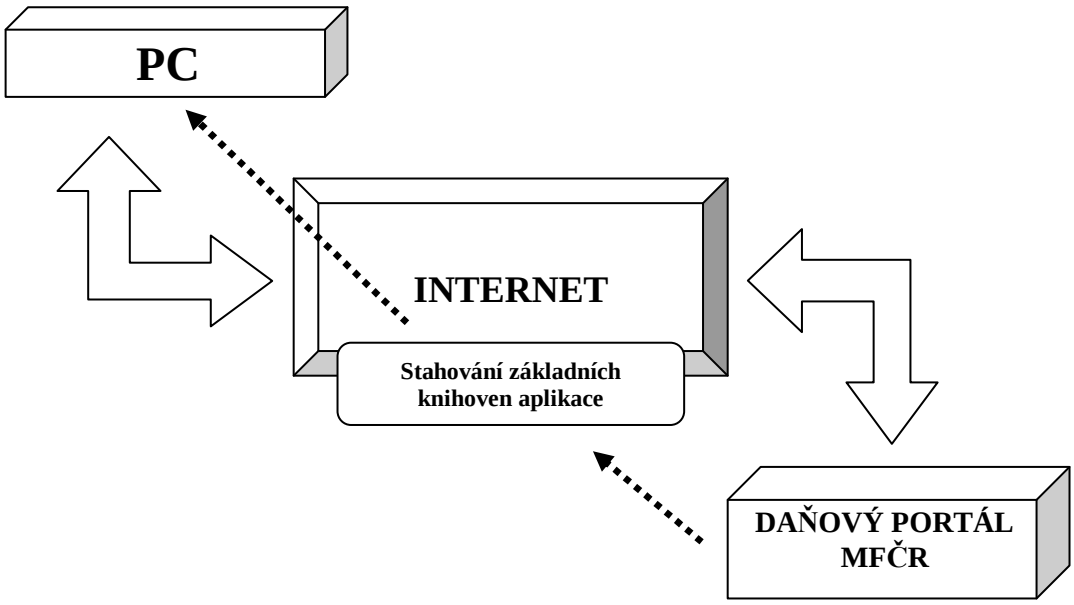
Obr. B 2: Zahájení podání



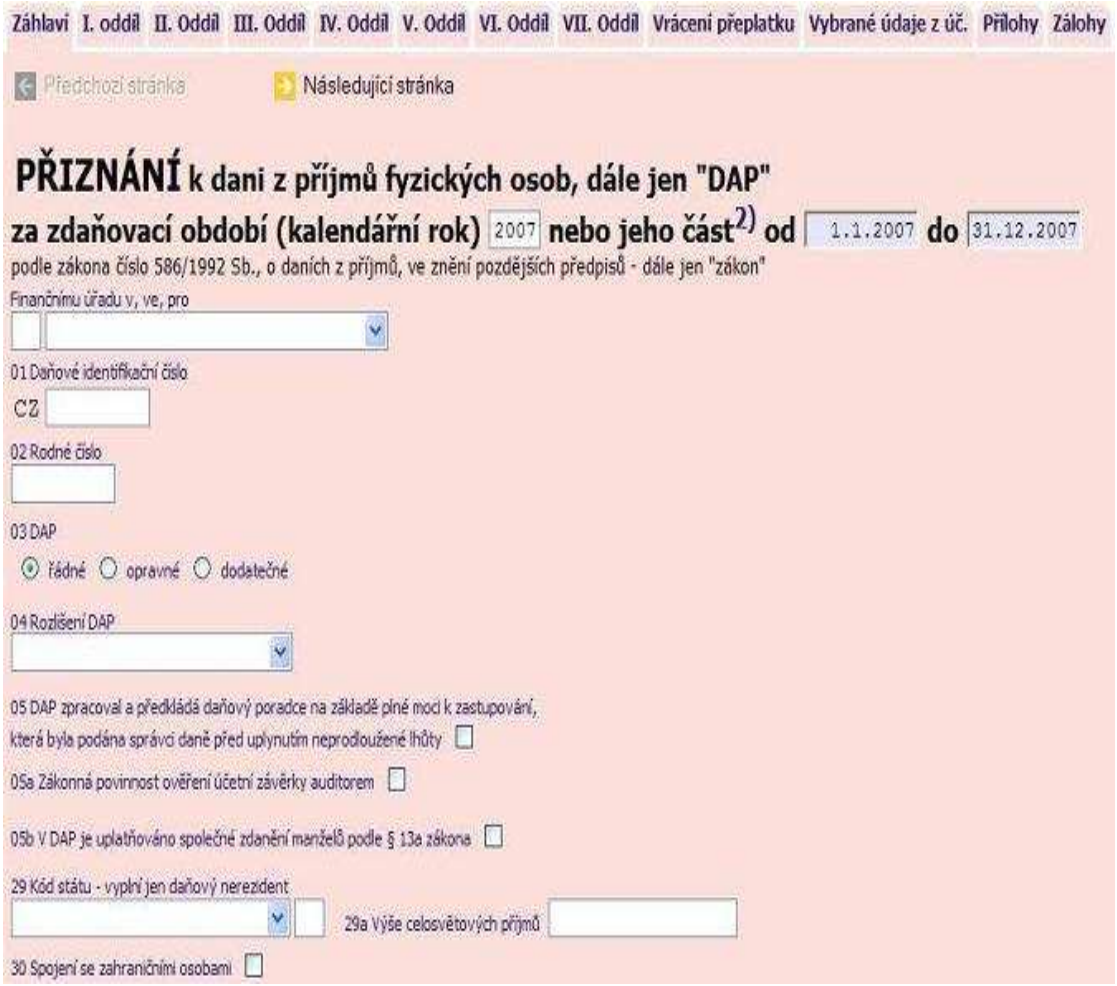
Obr. B3: Volba podání



Obr. B4: Stahování daňových programů

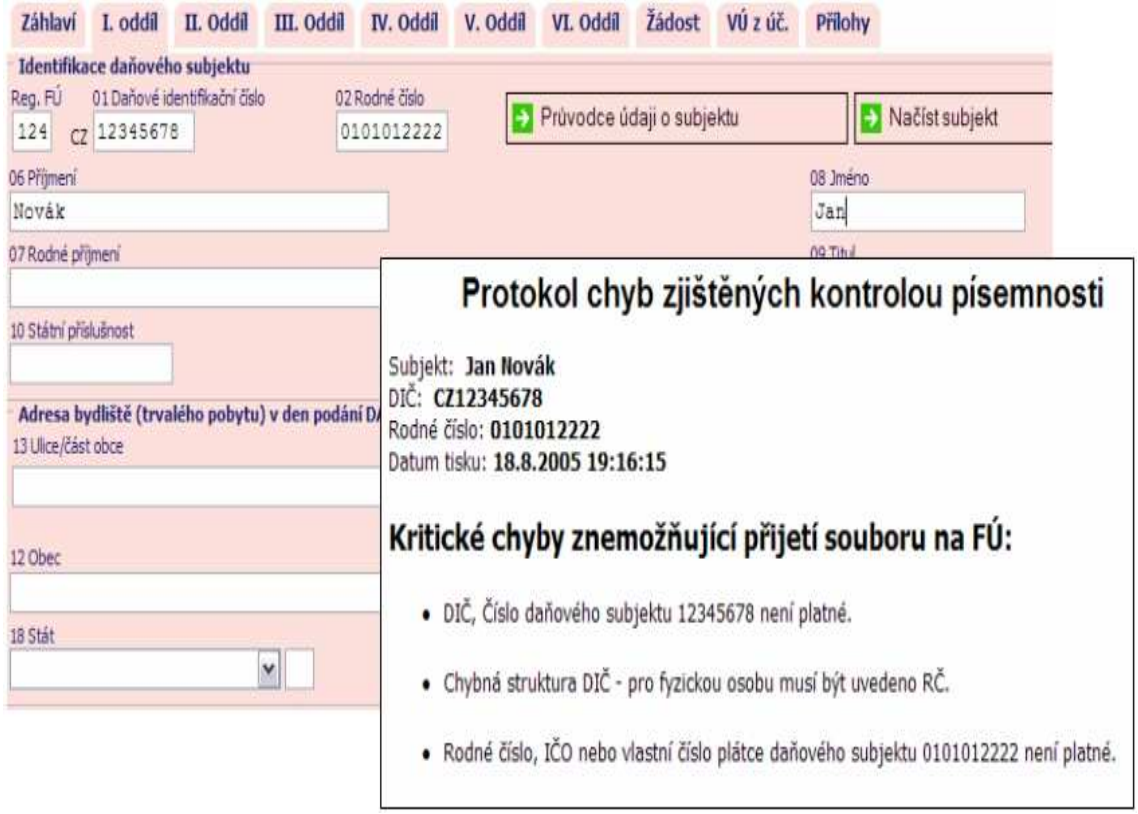


Obr. B5: Vyplňování daňového formuláře

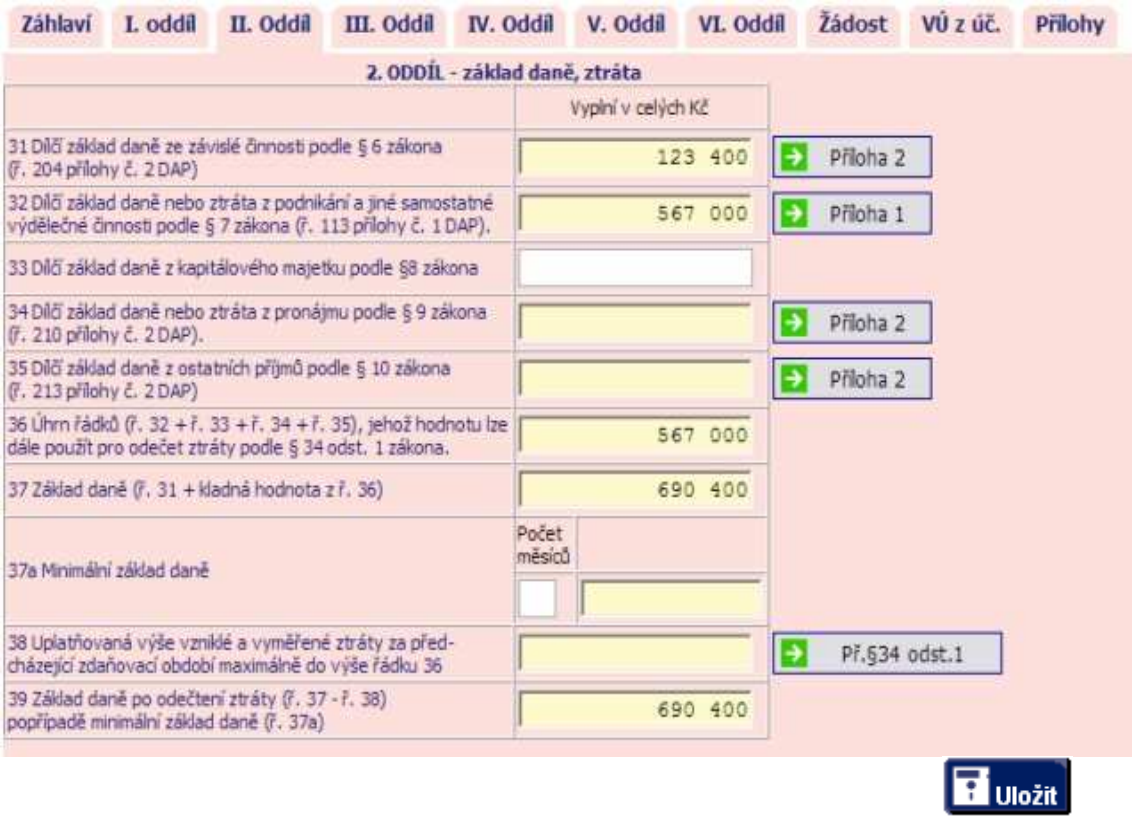


Obr. B6: Průvodce – pomoc s vyplněním

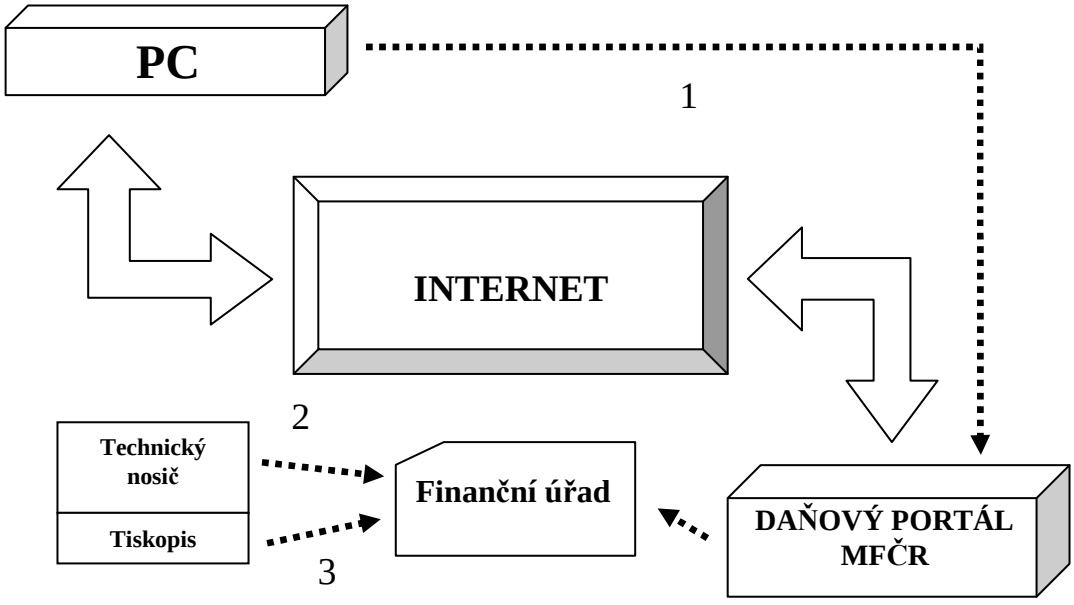
Obr. B7: Kontrola údajů



Obr. B8: Uložení rozpracovaného podání na vlastní PC



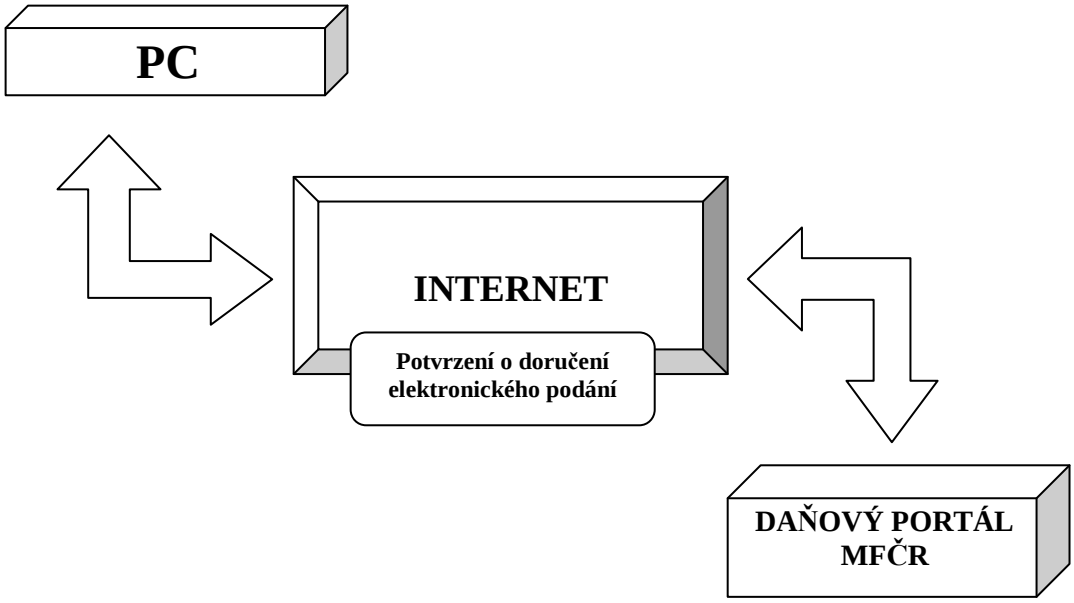
Obr. B9: Odeslání podání daňové správě



<u>Nabízí se 3 možnosti odeslaní:</u>

1) *Přímo z WWW prohlížeče*
2) *Pomocí technického nosiče*
3) *Pomocí tiskopisu*

Obr. B10: Potvrzení elektronického podání



Příloha C: ČIPOVÉ KARTY

VISA ELECTRON

Visa Electron od ČSOB je debetní elektronická karta s čipem. Jedná se o hybridní kartu, obsahuje jak čip, tak i magnetický proužek. Jed vydávána k účtům právnických i fyzických osob.

Obr. C 1: Visa Electron

Zdroj: *ČSOB* [online]. [2003], 2008 [cit. 2008-05-01]. Dostupný z WWW: <http://www.csob.cz>.

MAESTRO

Maestro od ČSOB je také debetní elektronická platební karta s čipem, jde opět o hybridní kartu. Tato je vydávána pouze k účtům právnických osob.

Obr. C 2: Maestro

Zdroj: *ČSOB* [online]. [2003], 2008 [cit. 2008-05-01]. Dostupný z WWW: <http://www.csob.cz>.

MASTERCARD INTERNET

MasterCard Internet je jediná karta od GE Money bank, se kterou je možno platit na internetu. Tato karta je určena výhradně k placení zboží a služeb na internetu.

Obr. C 3: MasterCard Internet

Zdroj: *GE Money : Česká republika* [online]. 2001-2008 [cit. 2008-05-01]. Dostupný z WWW: <http://www.gemoney.cz>.

EUROTEL KREDITNÍ KARTA STŘÍBRNÁ

Eurotel kreditní karta stříbrná je embosovaná kreditní karta karetní asociace MasterCard. Tato karta spolupracuje se Citibank a se společností Eurotel. Je bezpečnější oproti padělání a zneužití díky naskenované fotografií a podpisu držitele, které jsou „ zabudovány“ pod folií karty.

Obr. C 4: Eurotel kreditní karta stříbrná

Zdroj: *Citi* [online]. 2008 [cit. 2008-05-01]. Dostupný z WWW: <http://www.citibank.com>.

KREDIT + MASTERCARD GOLD

Kredit + MasterCard Gold je mezinárodní embosovaná kreditní karta České spořitelny pro fyzické osoby – klienty, kteří musí mít minimální čistý měsíční příjem 40 000 Kč. Její výhodou jsou vysoké limity čerpání (až 150 000 Kč/ 5 dnů pro bezhotovostní platby a 50 000 Kč/ 1 den), úvěrový limit až 500 000 Kč a různé druhy pojištění.

Obr. C 5: Kredit + MasterCard Gold

Zdroj: *Česká spořitelna* [online]. [2008] [cit. 2008-05-01]. Dostupný z WWW: <http://www.csas.cz>.

VISA PLATINUM

Visa Platinum je mezinárodní embosovaná karta od Živnostenské banky, která o ní uvádí, že je to nejprestižnější karta v ČR.

Obr. C 6: Visa Platinum

Zdroj: *UniCredit Bank* [online]. [2008] [cit. 2008-05-01]. Dostupný z WWW: <http://www.unicreditbank.cz>.

HVB PREMIUM CARD

HVB Premium Card je tzv. Černá karta HypoVereinsbank v Německu. Jedná se o exkluzivní kreditní platební kartu, která poskytuje mnoho výhod.

Obr. C 7: HVB Premium Card

Zdroj: *HypoVereinsbank : UniCredit Group* [online]. [2008] [cit. 2008-05-01]. Dostupný z WWW: <http://www.hypovereinsbank.de>.